Science and Mathematics Education Centre

Physical Security Professional's Body of Knowledge: a cultural domain analysis of physical security's knowledge structure

Michael P Coole

This thesis is presented for the Degree of
Doctor of Philosophy
of
Curtin University

May 2015

Declaration

This thesis contains no material which has been accepted for the award of any other degree or diploma in any university. To the best of my knowledge and belief, this thesis contains no material previously published by any other person except where due acknowledgement has been made.

Signature: 

Date: 10/05/2015

Reasoning behind the study

This study sought to overcome a dearth in understanding regarding knowledge required to be taught by institutions of higher learning, and mastered by professionals for security to move along the professionalisation path. The research evolved from a series of questions I had considered after commencing a teaching role within an Australian university. I had worked in both the military and civilian security environments for many years, and I had completed a Masters by Research degree in the area of security science. When I commenced teaching I asked myself what do I need to teach, what is essential and what is desirable, and what is the best way to teach security to undergraduate students? The reality is that there was no easy answer, as clouding the issue was the depth and breadth of security education.

Topics include criminology, terrorism, intelligence, management along with technology based units in intrusion detection, access control and closed circuit television (CCTV). Such depth and breadth in many security courses stems from significant diversity in the security domain's employment options for graduates. In addition, much of the security domain within the law and order paradigm (non-traditional) sits at the operational end of security's occupational stratum, with diminutive recognition for the professional category membership. Central to security's emergence and acceptance by both the public and legal arenas at the higher end of the stratum as a profession is its evidence of a valid body of knowledge that requires formal education through institutions of higher learning. Such knowledge must demonstrate how it brings about consistent and predictable changes in the environment to provide a state of being secure.

Consequently, I recognised the need to explore how the professional stratum of the security domain is jurisdictionally divided, each with its relevant knowledge requisites. Very quickly this exploration uncovered a project of significant scope. This led me to focus on physical security only, to map graduates' jurisdictional domain knowledge requisites, setting a framework for further sub-domain investigations. Accordingly, the study is not about technical details of locks or specific barriers, nor is it about alarm specifications and response personnel. The focus of this study was about the role physical security professionals play in the protection of assets and their requisite core and supporting knowledge in terms of a desirable curriculum model.

Abstract

Many new professions are emerging across contemporary society and as part of this societal transformation debate on the professional status of higher strata security personnel is intensifying. This debate is steered by the notion of the modern day security professional along with his or her claim of specialised occupational skills. Furthermore, many modern day professionals in security apply expertise in a specific jurisdictional field. Within the broad security domain, one specialised practising area is physical security which requires both general and specialised knowledge. However, a criterion of professionalism argues that physical security cannot be considered a profession, or progress along its professionalisation path, until its practice is based on an explicit body of knowledge and consistent educational standards. The study undertook a cultural domain analysis to articulate the physical security professionals' knowledge system, thereby isolating fundamental units and building a structure of knowledge.

The study applied a multiphase approach, (a) a literature critique to detect and localise repeated themes within the sub-domain, (b) expert interviews to enrich explicitly extracted knowledge concept categories, (c) quantitative validation to understand macro structure, and (d) focus group analysis for understanding the relationship between knowledge content and structure and educational goals. The study's findings demonstrate that a physical security body of knowledge comprises a matrix of task related knowledge categories. Such knowledge is broad and ranges from understanding the contextual threats, to using security theories and principles, to engineering knowledge of technical components which is supported by professional enabling knowledge. Furthermore, such knowledge has a hierarchical structure, organised based on the professional tasks of diagnosing the security problem, inference to reach the optimal resolution among many options, and finally, treatment. Such structure informs the teaching order of learning units to constructively build knowledge in a logical manner.

Acknowledgements

This thesis is dedicated to the men and women of the security domain in recognition of their tireless efforts to protect society from harm while also developing a professional basis in acknowledgement that one day security will emerge as a profession in the group phenomenon, thank you.

To my two supervisors, Professor David Treagust and Dr David Brooks who provided guidance and feedback in the design of the study, its development and its final outcomes: Thank you.

To the many security professionals who participated in the study, thank you for your time and important input, without which the outcomes of the study could never have been produced.

To my family who provided total support for this thesis from its proposal stage through to its completion, thank you for understanding.

Contents

List of Tables

List of Figures

Publications and conference presentations

Coole, M., & Brooks, D.J. (2011). Mapping the organizational relations within physical security's body of knowledge: a management heuristic of sound theory and best practice. Proceedings of the 4th Australian Security and Intelligence Conference, Edith Cowan University, Perth Western Australia.

Abstract

Security Science education at university levels is still in its infancy, with little agreement towards knowledge, curriculum and competency. Therefore it is essential that educators draw on relevant literature highlighting means of efficient and effective knowledge transfer for tertiary students within the security science domain. Such knowledge transfer will reduce the gap between academic knowledge (explicit) and professional competency (tacit knowledge) at the tertiary level. This paper presents phase one of a multiphase study.

A qualitative systems based knowledge structure of security domain categories has been conceptually mapped as a domain heuristic. The heuristic drew on research highlighting that experts have both richer depths of domain knowledge and superior cross referenced organizational structure than novices. The conceptual map takes a top-down approach bounded by routine activity, rational choice, situational crime prevention, defence in depth, security decay and management theories within the elements of prevention, preparedness, response and recovery. Results indicate that within a systems approach, core professional competencies relate to their ability to skilfully apply the theories and best practice principles represented within the preliminary heuristic that brings together academic theory with practising security strategies.

Coole, M., Brooks, D.J., Treagust, D. (2015). The Physical Security Professional: Formulating a Novel Body of Knowledge. Journal of Applied Security Research, 10(3).

Abstract

Debate on the professional status and what constitutes the security domain is intensifying. One practising area of security is physical security, which requires both general and specialised knowledge. However, physical security cannot be considered a profession until their practice is based on an explicit body of knowledge and consistent educational standards. Therefore, the study undertook a cultural domain analysis to articulate a physical security professionals' knowledge system, isolating fundamental units and structure of knowledge. The study applied a multiphase approach; conducting a literature critique, expert interviews, quantitative validation and focus group analysis.

Study findings demonstrate that the physical security body of knowledge is a matrix of knowledge categories. Knowledge is broad and range from facility contextualization to movement control to explicit aspects such as locks. Nevertheless, this knowledge has a hierarchical structure, organised based on the professional tasks of diagnosing the security problem, inference to reach the optimal resolution among many and finally, treatment.

Chapter 1: Study introduction

1.1 Introduction

Many new professions are emerging across contemporary society. However, for these professions their embryonic development is challenging, with clear argument that unless their underpinning knowledge base can be explicitly articulated no case exists for professional recognition. Emerging professional domains must therefore through evidentiary means uncover their knowledge base and convince the public of its complexity and necessity to be recognised in the group phenomenon. One such emerging domain is that of the security professional. However, security as an occupational endeavour is divided into two prominent domain streams; one denoted as traditional security and the other non-traditional security. Traditional security focuses towards concerns of sovereignty and the stability of nation states in the face of foreign national threats; this is pursued politically and militarily. The non-traditional stream of security considers other threat typologies across a vast array of societal concerns throughout the international community, or within the functioning of nation states.

Sitting within a nation's non-traditional domain stream is its security industry or sector. This stream is divided into a diverse range of distinct occupational category roles providing specific client centred protective services. It includes the broader practice area of physical security, and is what many citizens perceive when they consider or pursue day-to-day security. Within this embodiment are a strata of roles and activities and occupational services ranging from operational guard force and electronic security installers and integrators to security managers, and those persons providing highly complex protective advice across a broad range of corporate sectors.

However, indistinct understandings exist across non-traditional security's higher strata occupational categories relating to the services provided and their respective educational underpinnings. For instance, persons working in the upper sphere of the non-traditional stratum are referring to themselves as security professionals. Yet there is limited understanding of what constitutes a security professional, what their knowledge and jurisdictional basis is, and formal educational requirements supporting their services. As such, this study investigated the emerging sub-domain professional stream of physical security. Chapter One presents the background discussion framing this exploration. The

chapter draws on the Australian security professionals' discourse to seat a broader in-depth analysis of the professional knowledge required by practitioners in what is a pan-cultural practice stream.

Section 1.2 of the chapter presents the study's backgrounding pronouncing the context of the study. Section 1.3 conveys the significance of the study accordant with this discussion. This discourse is considered in the Australian context in Section 1.4 providing a folk basis for the study. Then Section 1.5 presents the study's seating as a pan-cultural domain analysis (cultural domain analysis). Section 1.6 introduces cognitive constructivism as the underlying theoretical frame of the study, and Section 1.7 introduces the study's research objectives and supporting research questions (Section 1.7.1). This discussion is summarised in Section 1.8 via a reflection and concludes in Section 1.9.

1.2 Background

A domain is defined as a particular area of activity or life, a field of knowledge or activity area (1981, p. 246); the scope of a subject, or an area of activity over which somebody has influence, or is controlled by a particular person or group. Extending on this is the notion of a cultural domain where culture is expressed as "the accumulated store of symbols, ideas, and material products associated with a social system, be it an entire society or a family unit" (Johnson, 1995, p. 68). In other words, it is a shared system of meaning (Spradley, 1979, p. 4), and a cultural domain refers to the fundamental units of cultural knowledge (symbols) for a specific domain organized accordant with a single semantic relationship, in terms of similarity and differences (Bernard & Ryan, 2010). The security domain within the context of this study is considered a distinct yet broad occupational cultural domain.

For the security domain, debate embodying the professional status of individuals within it is intensifying. Steering this debate is literature drawn from other domains, emphasising that a profession and its professionals are defined according to the status of their agreed body of knowledge, education standards linked to competencies aligned with such bodies of knowledge and the public's confidence as a result of such standards (Wilensky, 1964; Eraut, 1994; Abbott, 1998; Smith & Brooks, 2013). Yet to date there has been limited success in defining educational standards and course content across the

significantly diverse security domain. Such a lack in agreed body of knowledge and educational standards arguably leaves the security domain and specific practice areas within it lacking in public confidence and professional standing.

1.3 Significance of the problem

A review of the broad literature highlights the current debate recognising or rebuffing the notion of the security professional, or security as a profession will continue for some time (Nalla & Morash, 2002; Garcia, 2000; Rogers, 2000; Rogers et al, 2007; Borodzicz & Gibson, 2006; Anderson, 2007; Australian Interim Security Taskforce, 2008; Brooks, 2007; 2011; Coole & Brooks, 2011). At this time, identifying who or what delineates a security professional remains unclear (Horrocks, 2001, p. 226; Smith & Brooks, 2013, p. 243). The future development of professionalism in the security industry is dependent on the improvement of formal, structured programs that meet the needs of the security industry (Horrocks, 2001, p. 226; Smith & Brooks, 2013, p. 244) and society at the professional level. Johnston and Warner's (2014, p. 15) works call for more emphasis on physical security research, expressing that we need to start thinking about physical security as something that can be a highly scholastic research subject, pointing out that with more rigour we may actually achieve more effective physical security.

It is acknowledged within the literature on professionalism that before an occupation can be considered a profession, it must develop a clear and more solidified academic basis (Horrocks, 2001, p. 220; Axt, 2002, p. 142). This basis must include a well-defined and inclusive body of knowledge (Horrocks, 2001, p. 226) along with internal structure (Smith & Brooks, 2013, p. 245); as academic knowledge underpins and therefore legitimizes professional work (Abbott, 1988, p. 54), and this is so for the security domain (Horrocks, 2001, p. 220). Central to this discourse is the argument put forward by authors including Martin and Guerin (2005, p. 16) that a formal body of knowledge defines a professions' jurisdictional practice. A view also expressed by Morris, Crawford, Hodgson, Shepherd and Thomas (2006, p. 710) who stress that ownership of a distinctive body of knowledge is a vitally important element of any profession; this needs to be an inclusive body of knowledge containing concepts, principles and theories (Smith & Brooks, 2013, p. 1). Smith and Brooks (2013, p. 1)

highlight that this includes an internal structure of knowledge achieved through internal relationships between concepts so that consistency and logic prevail.

Smith and Brooks (2013, p. 245) considered that evidence based research will play an important role in the professionalisation of security. Within this examination is a focus on higher education in providing the necessary abstract knowledge for future security professionals, denoted by Phinney and Smith (2009, p. 1), Coole and Brooks (2011, p. 1) and Smith and Brooks (2013, p. 1) as security science. As the writings of Gillespie (1981, p. 371) highlight, university is the focal point of professionalism and this needs to be taught through the existence of a recognised academic base (Horrocks, 2001, p. 220). Within this context, the Collins Dictionary (Krebs, 1981) defines science as: 1. "The systematic study of the nature and behaviour of the material and physical universe based on: observation, experiment, and measurement. 2. The knowledge so obtained or the practice of obtaining it. 3. Any particular branch of this knowledge: the applied sciences. 4. Any body of knowledge organised in a systematic manner. 5. Skill or technique. 6. Arch. Knowledge" (p. 1163). The Collins Dictionary further defines a profession as 1. "An occupation requiring special training in the liberal arts or sciences, or, 2. The body of people in such an occupation (p. 1029)".

These combined definitions highlight that for the security domain or individuals within it at a group level to be considered professionals, they must have organised knowledge, learned through training in the arts or sciences, or both, commensurate with their areas of foci. Thus, accordant with the writings of Axt (2002, p. 142), such knowledge needs to be communicated to higher education towards establishing standards upon which to base their qualifications programs. Both prospective professionals and the broader public rely on uniform standards of education to develop dependable expectations regarding any profession and its competencies (Fox, 1994, p. 202). Although, deferring here to the writings of Allan (1996, p. 1), educational objectives are multifaceted, where the design of learning experiences for higher education has shifted towards more outcomes led objectives. Both Tyler (1949) and Allan (1996, p. 94) emphasise the importance of supporting learning objectives, stating:

> If an educational programme is to be planned and efforts for continued improvements are to be made, it is very necessary to have some conception

> of the goals that are being aimed at. These educational objectives (goals) become the criteria by which content is outlined, materials are selected, instructional procedures are developed and tests and examinations are prepared (Tyler, 1949, p. 3).

To date, there are no agreed on or research supported educational objectives for security professionals including those physical security practitioners. As the Hallcrest report (Cunningham & Taylor, 1985) acknowledged, the field of security itself constitutes a specialized knowledge, but it is questionable whether in the traditional academic sense security can be considered a body of knowledge that is girded with a strong academic basis. Expounding the lack of research supported basis for the security industry, the role of education is premised to be looking at the field from a distance, from an objective position, to conduct research, analyse, be critical, develop theory and support change and innovation (Cunningham & Taylor, 1985, p. 227). This view still stands today.

The paucity of validated security curriculum highlights that changes are needed; changes which must be made on the basis of validated information. As Criscuoli (1988, p. 99) points out, up-to-date knowledge of physical security devices and controls along with their uses are the obvious knowledge requirements for physical security professionals; what is not obvious is the scope and breadth of the subject. Thus, a cultural domain analysis focusing on taxonomic structure can provide professional comprehension in terms of informing the development of higher educational curriculum for future physical security professionals. As such, the outcomes of the study included;

- A consensual map representing the organisational structure of knowledge concepts within the domain of physical security;
- A domain heuristic for articulating the occupational role knowledge areas and supporting knowledge concept categories within physical security's knowledge base;
- Visual clarity for security professionals to understand where their particular expertise fits into the physical security domain within a systems approach;
- A means of explicitly presenting (reception learning) the hierarchical knowledge areas and their subordinate concepts of physical security to tertiary students as a richly cross-referenced organised structure enhancing their efficiency of learning;
- The development of a learning objective for physical security professionals;

- Guidance for integrating physical security theory with best practice principles; and
- Contributing towards developing the consensual knowledge and professional competencies for physical security educators in institutions of higher learning.

The significance of this study lies in its symbolic outcomes, as it is argued that the concept of the security professional will be better understood through research driven domain exploration. Such an outcome would enhance the professional status of security through validated higher education curriculum and associated competency measures, thus increasing the broader public's understanding and confidence in their services. Consequently it is argued that the professional status for the domain will not advance until the necessary research, such as this, is undertaken to provide the underpinning articulation and relevant body of professional knowledge. Such an outcome is essential towards increasing the public's confidence in the security profession and facilitating the pronunciation of the security professional underpinned by validated instructional process (Phinney & Smith, 2009, p. 2).

Nevertheless, the task of identifying and analysing a cultural domain is considered difficult, as many participants within do not visibly divide their field into clear, discrete words in categories based on relationships of inclusion. In addition, for many within a professional area (domain), their knowledge is tacit, outside everyday awareness (Spradley, 1979, p. 102). Yet, all cultural domains demonstrate a formal structure represented by a cover term, defined as the name of the domain or category which includes smaller categories; this represents a broader name for a category of cultural knowledge. Second, all domains have two or more included terms, which are folk terms that belong to a category of knowledge encompassed by the cover term. Then, a single semantic relationship exists which links the cover term to all the included terms in its set (Spradley, 1979, p. 101).

Furthermore, all domains have boundaries, where some terms belong inside the boundary, and others belong outside the domain set (Spradley, 1979, p. 102). A cultural domain analysis is based on three broader elements of the research enquiry, which includes setting the professional boundary, and identifying and isolating the fundamental units of cultural knowledge within this boundary. Establishing a taxonomy

shows their relations, which highlights subsets, which further highlights how these subsets are related to the domain as a whole. Then an interpretation of these subsets is undertaken in relation to the goal of the enquiry (Spradley, 1979).

1.4 The security domain

Security is well recognised as an occupational domain discipline within contemporary society. However, as an emerging profession, security, and specifically security education, as a contemporary discourse is a complex issue discussed by a broad range of authors (Manunta, 1999; Rogers, 2000; Kicinger, 2004; McCrie, 2004; Wang, 2005; Borodzicz & Gibson, 2006; Brooks, 2007; Rogers, Palmgren, Giever & Garcia, 2007; Zietek, 2008; Stone, 2009; Brooks, 2010; Griffiths, Brooks & Corkill, 2011; Coole & Brooks, 2009; 2011) as it encompasses concerns involving traditional (threats to sovereignty) and non-traditional (threats to law and order) endangerments rendered across many organisations including government operations, military, law enforcement, emergency services and private security operations (McCrie, 2004, p. 12; Wang, 2005, pp. 1-3). Within the non-traditional domain Manunta (1999, p. 60) associates the discourse's focus towards managing those threats which pose a risk accordant with the functioning within a nation state, with roots spreading from natural disasters to crime prevention within the concept of law and order.

Talbot and Jakeman (2009, p. 55) noted that threats encompassed within the crime prevention paradigm are faced by governments at national, state and territory levels, commercial enterprises, individual groups and persons. They explain that in this paradigm context, physical and procedural measures are designed and implemented to protect intangible assets or capabilities from defined threats. It is further acknowledged that these measures are used by both government agencies and the corporate sector to mitigate contextual threats that pose a risk to objectives (Borodzicz & Gibson, 2006). Such measures stem from the physical security sub-domain (Talbot & Jakeman, 2009, p. 55; Smith & Brooks, 2013). Within this sub-domain, Nalla and Morash (2002) emphasised there are many complex tasks requiring high level decision making, however they acknowledge a public perception that much of the security domain is a simple occupational enterprise. They argue that the public sees security primarily

consisting of security guards or barriers, resulting in a misunderstood domain at the higher end of the professional continuum.

The complexity of the professionalism discourse is recognised by Manunta (1999, p. 57), who outlined the 21st century's academic challenges for the emerging profession of security, stating:

> We security professionals and scholars are entering the millennium from a very flimsy position: We lack a robust and workable definition of security; Our positions are questionable from the viewpoints of understanding, judgement, methodology and ethics…arguably, no professional in any other field is so vulnerable to malicious attacks-and this weakness is perhaps the best evidence that security management is still not a profession. (Manunta, 1999, p. 57)

Manunta's view is supported in the later work of Borodzicz and Gibson (2006) who express that the mere concept of security can have different meanings depending on context. Such a variegated domain has resulted in diverse and multi-disciplinary occupational strata, concerning a wide spectrum of activities and skills (Brooks, 2007, p. 1). Such diversity results in a significant breadth of topics with which domain professionals need to be familiar (Nalla & Morash, 2002) due to a lack of jurisdictional boundary. Coole and Brooks (2011, p. 1) believe this very issue drives security's lack of professional consensus in both definition and professional standing. Nevertheless, Anderson's work (2007, p. 1) highlights that the current profile of the security profession (non-traditional) is undergoing significant change. It is acknowledged that in contemporary times professionals have become essential to the very functioning of society, as in the words of Donald (1983, pp. 3-4), "we look to professionals for the definition and solution of society's problems".

Part of the security domain's change encompasses discourse towards clearly defining the concept of the security professional and identifying core professional competencies, declared by Griffiths, Brooks and Corkill (2011, p. 3) to include both "academic and practical" aspects. This is a view supported earlier in the writings of Abbott's (1988, pp. 7-8) who articulated that professionals competently apply abstract knowledge to

particular cases to solve society's problems, which requires special abstract skills developed through specialized training. An Australian government sponsored body in the current discourse, the Australian Interim Security Professionals Task Force (2008, p. 6;) identified contemporary security professionals as those groups of people working at the senior end of the operational sector and in the strategic sector of the security industry. However, this definition is vague, and the Task Force did not articulate professional practice areas linked to competency measures within this definition.

Nonetheless, the Task Force acknowledged that security professionals as a group are critical in supporting the protection of government, commercial organisations, non-government organisations and the community against threats to the functioning of society. The Task Force conceded that security professionals have not been able to contribute their full potential to the nation's security and safety primarily due a lack of clear understanding of either security professionals or the profession. Nevertheless, the Task Force emphasized the point that security professionals still have a responsibility for ensuring that all aspects of their work are soundly based in theory and established practices (2008, p. 9). This leaves the question that Wang (2005, p. 7) asks in the traditional domain...How do we combine theory with practice? To such a statement, the Task Force did not provide the basis for such an approach, and as Brooks (2007, p. 2) highlights, traditionally security practitioners have focused on their niche areas.

One arguable barrier in clearly defining a security professional is a lack in consensual body of knowledge and agreed educational standards (Smith & Brooks, 2013, pp. 1-2) underpinning their designation. Knowledge relates to that which can be clearly stated...verbally articulated (Jaques, 1989, p. 34), and is defined by the Collins Dictionary (Krebs, 1981, p. 698) as: "(1) the facts or experiences known by a person or group of people, (2) the state of knowing, (3) consciousness of familiarity gained by experience or learning, (4) erudiation of informed learning, (5) specific information about a subject, and (6) understanding". As Jaques (1989, p. 34) expressed, if you cannot state it, you do not know it. Thus, if the knowledge underpinning the security professional cannot be stated, it is arguably not held.

Congruent with Jaques' views, Abbott (1988, p. 324) wrote that all kinds of knowledge (that which can be stated) are organisable as common resources for a body of

individuals. Such a resource is considered a "professional's formal knowledge system" (Abbott, 1988, p. 53) articulated by Martin and Guerin (2005, p. viii) as "a body of knowledge, defined as the abstract knowledge needed by practitioners to perform the profession's work". Yet as Rogers, et al. (2007, p. 2) and Brooks (2007) point out, Security education at a university level is in its infancy, with little agreement towards curriculum, knowledge levels, and arguably competency indicators.

Nonetheless, it is acknowledged by McCrie (2004, p. 17) and the Australian Interim Security Professional's Task Force (2008, p. 10) that security has created a body of knowledge. However, authors including Manunta (1999), Horrocks (2001), Rogers, et al. (2007, p. 1), Brooks (2007, p. 7) and Griffiths, Brooks and Corkill (2011, p. 4) refute its cohesive existence. Nevertheless, in order to develop a definition of security, Brooks (2007, p. 5) conducted a study identifying 14 hierarchical security subject categories representing many associated industries across many occupations, highlighting the salient practice areas in which security as a discipline draws its body of knowledge (See Table 1.1)

Table 1.1 Hierarchical security domain subject categories of Brooks (2007)

Security domain subject category descriptors		
Criminology	Business continuity management	Fire science
Facility management	Industrial security	Information & computer
Investigations	Physical security	Security principles
Risk management	Safety	Security law
Security management	Security technology	

However, these categories are broad in nature and lack content and structure. Therefore Brooks (2010, p. 237) recommended further research in the form of psychometric multidimensional scaling to create a concept map of security knowledge categories and relationships towards developing deeper understanding of the domain. This arguably would lead to a jurisdictionally valid curriculum and clearer competency requirements for future security professionals.

1.4.1 The Australian non-traditional security context

Security is recognised as a primary concern for modern-day societies (Sarre & Prenzler, 2009, p. ix) where the growth of private security within the context of law and order is a transnational phenomenon (Prenzler & Sarre, 2012, p. 38). Australia has a stake in this phenomenon; combined across all sectors in Australia security supports the protection of government assets, commercial organisations, non-government organisations and the greater community (Australian Interim Security Professionals Task Force, 2008, p. 6). Today within Australia, as with global trends, the self-provision of security for corporations and individuals is reflective of the acknowledged repayments from prevention measures. Such measures have been achieved through situational and environmental design crime prevention techniques and principles (Prenzler & Sarre, 1998, p. 2).

Situational crime prevention as a concept is a salient basis for much of the non-traditional security domain, and is defined as: "opportunity-reduction measures that are (1) directed at highly specific forms of crime, (2) that involve the management, design or manipulation of the immediate environment in as systematic and permanent way as possible, and (3) so as to increase the effort and risks of crime and reduce the rewards as perceived by a range of offenders" (Clarke, 1992, p. 4). Clarke (1992, p. 5) expresses that situational crime prevention thinking is a problem centred approach, analysing and defining the crime problem towards identifying and testing possible solutions, evaluating results, and where necessary repeating the cycle until successful. Physical security falls out of situational crime prevention theory (The American Institute of Architects, 2004, p. 45; Kiszelewska & Coole, 2013, p. 2; Lab, 2014, p. 219) and is complimented through environmental design theoretical underpinnings (The American Institute of Architects, 2004, p. 45).

As with the criminological approach, it is also acknowledge that the problem-centred approach is employed when conceptualising physical security requirements (Garcia, 2008, p. xvii). This approach focuses towards defining and understanding the security problem prior to designing and then evaluating the protective mitigation system (Garcia, 2008, p. xvii). Clarke (1992, p. 7) indicates this is a pan-cultural approach and can be utilized within any organisational or management structure that can amass the resources and dynamism to address crime problems. Extending this approach is the concept of environmental design in reducing opportunities for crime. This approach involves designing the built environment to reduce the opportunity for, and fear of crime and disorder. Such an approach takes advantage of natural opportunities to control access, increase opportunities for non-technical surveillance and establish territorial reinforcement (Atlas, 2008, p. 3). Combined situational crime prevention and crime prevention through environmental design (CPTED) theory provide an initial theoretical basis for physical security.

Within the criminological paradigm, Prenzler and Sarre (1998, p. 2) argue that security becomes an umbrella term including synonymous terms such as “risk management, asset protection and loss prevention” and is now recognised as a highly diverse role that can be provided through a variety of mechanisms and sources to reduce deviance within a given context. These authors state that in Australia the private and public security industry involves a vast mosaic of occupational functions (Table 1.2) associated with both situational and environmental design approaches and investigations to reduce the incidence of deviant acts. Within this diverse range of strategies and their underpinning occupational categories, Prenzler and Sarre (1998, p. 2) further emphasize a stratum of responsibilities where different roles require different levels of technical or interpersonal skills to address the relevant societal problems according to context.

Table 1.2 Australian security contributors (Prenzler, Earle & Sarre, 2009, p. 3)

Security Providers, 1996-2006					
	1996	2001	2006	% change 1996 to 2006	% of total 2006
Private investigator	904	1,205	761	-16	1.4
Security consultant	584	733	894	+53	1.7
Locksmith	1,492	1,877	2,279	+53	4.3
Insurance investigator	401	486	418	+4.2	0.8
Debt collector	5,933	9,666	10141	+71	19.2
Court bailiff or sheriff	566	600	694	+23	1.3
Armoured car escort	53	88	485	+815	0.9
Security officer	27,439	33,884	5,424	n/a	10.3
Alarm, security or surveillance monitor	n/a	n/a	30,752	n/a	58.3
Crowd controller	n/a	n/a	920	n/a	0.5
Total security	37,372	48,579	52,768	+41.2	
Police	39,225	41,426	44,898	+14.5	
Population	17,752,829	18,769,249	19,855,288	+11.8	

Within this industry mosaic is a complexity of tasks undertaken across various occupational groups, including operational roles such as surveillance, investigations, crowd control, prison escorts and court security, guarding and patrolling; along with proactive crime prevention, risk management and assessment, weapons training, crime scene examination, information technology, technology systems development and communications support (Prenzler & Sarre, 2009, p. 1). Such diversity and growth has reached a point where private security personnel outnumber sworn police by more than two-to-one (Prenzler, Earle & Sarre, 2009, p. 1), where their foremost focus is still towards crime prevention and the enforcement of laws (Prenzler & Sarre, 1998, p. 2)

Such depth and breadth of the Australian security industry makes it difficult to measure (Prenzler, 2005, p. 53). Internationally, according to Prenzler and Sarre (2012, p. 38), a 2011 survey across 70 countries estimated that around 19.5 million people were employed in private security duties, with an extended estimate of 25.5 million people across all countries. In addition, the entire industry was valued at $US 100-165 billion per annum, with an annual growth rate between 7-8 per cent. The Australian context is no different, with private security being a dynamic and rapidly evolving sector of the

Australian economy (Sarre & Prenzler, 2009, p. ix). This sector includes commercial contractors and in-house private security personnel (Prenzler, 2005, p. 53) as a large number of government agencies, businesses and educational enterprises employ their own security staff.

Nevertheless, in Australia there are three ways in which the private security industry can be measured, each with their own limitations. The federal government's Australian Bureau of Statistics (ABS) census survey conducted every five years, questions individuals regarding their main sources of employment. The ABS Labour Force Surveys gather occupational data based on employer reports on staff numbers and finally the industry licencing figures across licencing categories (Prenzler, 2005, p. 53) also yields valuable data. Table 1.2 presents tabulated figures indicating increased trends across occupational security categories in ABS census reports from 1996, 2001, 2006 to 2011, indicating the depth and breadth of the Australian security industry occupational categories.

1.4.2 The modern day security professional

Consistent with the public's perceptions (Nalla & Morash, 2002) a vast array of occupational groups, comprising the immense operational security industry in Australia, are presented in Table 1.2. However, lacking from this data set is the acknowledged occupational stream of the modern day security professional. Congruous with Table 1.2, the Australian Interim Security Professionals Task Force (2008, p. 4) offers the security continuum with security personnel working in the tactical, operational and strategic sectors of the industry. Nevertheless, it was emphatically acknowledged by the Task Force that there exists within this continuum a lack in understanding for those described as security professionals, stating:

> This lack of understanding is driven by ubiquitous understanding by security users of the difference between the quality and capabilities expected by those providing front-line operational services including manpower and technology, and those providing 'professional services security advice' such as security advisors and risk managers. (Australian Interim Security Professionals Task Force, 2008, p. 4)

The task force added that this position is further exacerbated by a lack of standards defining the expected knowledge, competencies and ethical behaviour of security professionals (p. 4), even in light of the acknowledgement of the requirement to promote the professional element of the security services stratum (p. 6). The Security Professional's Task Force's (2008, p. 4) viewpoint was more recently acknowledged in an Independent Commission Against Corruption (ICAC) report into corruption within the New South Wales (Australia) security industry. The report noted that the role of the security expert in achieving security project outcomes was rarely clearly defined, potentially leading to corrupt practices within the industry (ICAC, 2013).

Such persons are theoretically required to take responsibility for security projects and programs in the most far-reaching sense; "they provide significant input into the shaping of security decisions and the environment in which the security system functions" (Security Professional's Task Forces, 2008, p. 9). Within the literature it is acknowledged that the professions have had a short history in Australia, and not all emerging professions are classified by the Commonwealth Statisticians (Boreham, Pemberton & Wilson, 1976, p. 44), as is the case with the security professional. This lack of understanding of the security professional means this category of persons is neither recognised nor understood by Commonwealth Statisticians and the general public. As one participant in the study stated:

> When people ask what I do on a Saturday night, they say well what's that (security professional), a security guard? Also, I have to write down on all my forms that I'm a security engineer otherwise they don't know what I am. (Sharne)

Nevertheless, within Australia's occupational security categories (Table 1.2) is a specific statistic of interest for the study, an increasing number of security consultants from 584 (1996) to 894 (2006), the closest occupational group with regards to the Task Force's professional services security advice category including security advisors and risk managers. Again, this is a point supported in the ICAC report (2013) into corruption into the NSW security industry. The report expressed the view that for the electronic security industry there were three main participants; namely suppliers, installers and consultants. According to the ICAC report, suppliers sell electronic

security systems components to installers, installers or integrators integrate and supply various products to meet client requirements. However, consultants provide expert advice on security solutions based on customer needs and budget requirements.

From an international perspective, the American Institute of Architects (2004, p. 184) states that "security consultants provide management consultancy services specialising in security; loss prevention or security training; and security equipment system design, evaluation, and specifications". Their work explains that some security consultants also provide architecture and design services to clients and architects. The focus is to determine the security-related needs of their clients and to provide advice, information, and recommendations to clients; they offer their services by market or industry, by type of service, or by type of asset to be protected (p. 184).

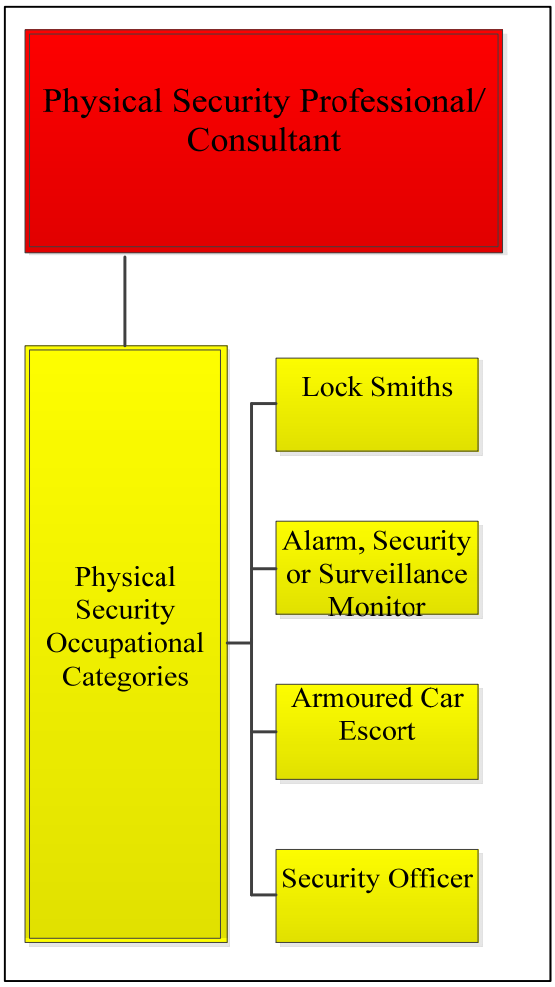
Fischer, Halibozek and Green (2013, p. 91) support the designation of security consultants as security professionals stating, "Security consultants are the professionals of the field, because they are paid for their professional opinions". Nevertheless, such professionals can go by other names, where professional security advisors are positioned within the corporate security paradigm. Corporate security is a sector within the greater security domain that provides internal security services and functions within either public or private enterprises in their pursuit of security (Brooks, 2013, p. 2). For example, in the corporate security context such advisors are also known as Protective Security Advisors, a term used by the Australian Government for their various departments in-house security advisors. In addition to this articulation of the security professional the works of Sennewald (2013, p. 1) acknowledge the security executive or in-house security consultant as a security professional. Sennewald states:

> As a full time salaried employee, the security executive of a given corporation serves in some measure as a proprietary or in-house consultant to senior-level management. He or she recommends appropriate and cost-effective strategies to achieve a wide variety of security objectives, loss control, crime prevention and investigative goals. (Sennewald, 2013, p. 1)

Sennewald (2013, p. 1) draws on the American Heritage Dictionary in supporting his notion, defining a consultant as (1) a person who gives expert or professional advice, (2) a person who consults another. Furthermore, Sennewald extends this view, explaining consulting as a problem solving process. In this process, the consultant must first identify the problem, gather available data pertaining to the problem, analyse the data, and then offer advice in the form of recommendations that will solve, or otherwise minimize, the problem (2103, pp. 6-7). Such views were expressed by Argyris and Schon (1974, p. 158) who, articulated that a professional must develop his or her own theory of practice which enables him or her to understand contextual, unstructured information presented by the client, sense which pieces are central or peripheral to the problem, to steer his or her professional behaviour in terms of outcome.

Further supporting this broader group's articulation as professionals are the writings of Abbott. Abbott's (1988, p. 8) work emphasized that for professionals the physical techniques themselves may be delegated to other workers (occupational groups) and that it is this very point that makes them professionals. Professionals control the abstractions that generate the practical techniques that solve society's professional problems. Thus, the professional security advisors themselves are not locksmiths, alarm security or surveillance monitors, or security officers (Table 1.2), but rather provide the professional advice in relation to security policy development and governance, along with control selection and the necessary decision making to meet contextual risk reduction requirements (Kiszelewska & Coole, 2013, p. 2). Therefore, they must sit within a stratum (Figure 1.1), integrating the many occupational category's outputs into a cohesive system commencing from a top-down approach, starting with a policy to protect and develop the appropriate systems to achieve said policies based on their understanding of the professional problem.

Figure 1.1 Security professionals/consultants and their supporting occupational categories

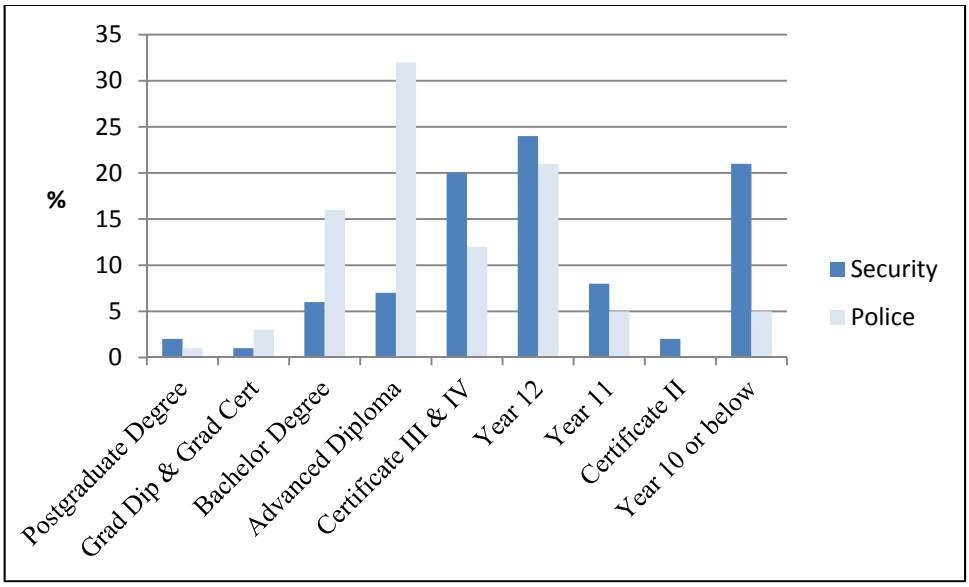


It is perhaps within this context that the security consultant or advisor can be articulated as the security professional. Yet to date, limited data exists for such persons, especially in terms of education, qualifications and area of foci. A United Kingdom survey across all security occupational groups of the security industry by Gill, Howell, Mawby and Pease (2012, p. 24), found that 34.3% (n=48) had a post graduate qualification, and 24.3% (n=34) had a university degree. This sample included the closest category to security professionals by the Australian designation, referred to as security specialists articulated as clients, demarcated as those persons who buy or manage security services (n=151). However, the study's results did not state specific areas of academic study. But, to date, limited official employment, experience and qualifications data exists for such persons.

While private security personnel out number their policing counterparts, it is pointed out by Prenzler, Earle and Sarre (2009, p. 5) that they are less likely to have obtained

tertiary education qualifications than their policing counterparts (see Figure 1.2), they earn lower salaries and they are more likely to be employed part time. Nonetheless, congruent with the concept of the security professional, Figure 1.2 does highlight the fact that for postgraduate level degrees security personnel were shown to be numerically more represented than their policing counterparts. These data indicate support for the premise that at the higher strata of the security continuum there does exist those persons with higher education qualifications who are employed in highly complex security advice activities.

Figure 1.2 Security education standards in Australia (Prenzler, Earle and Sarre, 2009)



The focus of this study is towards the physical security professional within the context of the contemporary security professional. That is, those persons at the higher strata of the operational sector and in the strategic sector of the security industry (Australian Interim Security Professionals Task Force, 2008) who specialise in providing a problem-centred approach to the physical protection (physical security) of assets. However, Johnston and Warner (2014, p. 13) question whether physical security has validity as a real field. They acknowledge physical security's 10,000 year plus history, its immense number of practitioners and the importance of physical security to a community's wellbeing. However they suggest that for the area to progress there needs to be an acceptance that physical security is a highly scholarly subject, with more

qualifications available at a tertiary level underpinned by more rigorous research. They openly question: Where are the degrees in physical security?

Nonetheless, physical security professionals are potentially represented as security consultants (Table 1.2), or security clients (Gill, Howell, Mawby & Pease, 2012, p. 24) and protective security advisors. In outlining and articulating their support for the concept of the security professional, the works of Horrocks (2001, pp. 1-2) and Axt (2002, p. 142) put forward the argument that the security domain must pursue the establishment of and enforce unambiguous qualifications criteria. This viewpoint was supported by the findings from Security Professional's Task Force (2008, p. 11), which acknowledged that standards defining the security professional were necessary, stating, "standards are concerned both with professional competencies and with working methods, practices and procedures". Consequently The Task Force presented four potential frameworks to be drawn on for establishing professionals' practice standards, which include:

1. Alignment with the Australian Qualifications Framework (AQF);
2. Certification levels based on responsibility and competence;
3. Role-based requirements framework; and
4. Alignment with Security Risk Management Body of Knowledge (SRMBOK) (Talbot & Jakeman, 2009) practice areas and activity areas.

These frameworks provide a potential basis for understanding security professionalism and more specifically, the concept of the security professional within the broader security domain. Equally, potential alignment with the Australian Qualifications Framework (AQF) emphasizes both educational standards and an educational hierarchy within the Australian security professionals' literature. Such hierarchies included security related roles aligned to educational attainment levels commencing with Certificate II qualifications (Guards) and progressing upwardly to include Doctor of Philosophy (PhD) level (Technical Specialist or Senior Consultant) (Australian Interim Security Professionals Task Force, 2008, p. 29).

Nonetheless, within these frameworks the Task Force only stated educational bands; it did not specify the knowledge areas and their supporting content aligned with and

required to reflect competence at any defined level. In addition to alignment with the AQF, the Task Force highlighted certification levels based on responsibility and competence. But certification is not education, and again a reasonable question asks, what are the knowledge requirements for levels of responsibility? This view is supported in the work of Sennewald (2013, pp. 8-9) who asserts that educational credentials are separate from professional certifications, which follow after education.

Sennewald (2013, pp. 8-9) holds the view that for a consultant argued to be a security professional, a two year college education should be the minimum for practice. However, ideally security professionals or consultants should have a Bachelor's Degree in the security profession, in either security administration, security management, administration of justice, police science, electrical engineering or technology, or architectural design. In light of the fact that the majority of people in senior managerial or executive positions to whom the consultant (professional) seeks to advise have earned degrees, many expect the specialist to be similarly educated (Sennewald, 2013, pp. 8-9). Sennewald contends:

> We live in a world in which credentials are mandated…An attorney, accountant, teacher or registered nurse has a clearly defined path of preparation to follow to earn that title. That is true with virtually any occupation. If a person deviated from the prescribed preparatory steps, yet claimed to be say, an engineer, that person could be viewed as a fraud. (Sennewald, 2013, p. 9)

In considering the relevance of education, The Australian Interim Security Professionals Task Force also highlighted role based requirements and alignment with the Security Risk Management Body of Knowledge (SRMBOK) of Talbot and Jakeman (2009). Consequently if such an alignment is accepted, the question is posed, what are the knowledge areas and their content that underpins professional competency, as the explicit roles for a physical security professional are not articulated at any agreed level? This is in light of the fact that Zipser's (1999, p. 1) works highlighted that professionals' standard of care in exercising their professional work will be judged according to the standards of a reasonably competent qualified person holding that skill. Nevertheless, these four frameworks present a starting point for professional consideration. However,

there does not exist research to support clear jurisdictional knowledge areas, content and syllabus structure, which align to roles, responsibilities and professional competencies. Nor is there research indicating how these jurisdictionally fit into the broader security domain, and couple with institutions of higher education.

On the other hand, SRMBOK (Talbot & Jakeman, 2009) does provide an initial means of articulating practice areas for professionals for whom knowledge areas and supporting content can be explored, and these practice areas were loosely aligned with the AQF (Australian Interim Security Professionals Task Force, 2008, p. 29). For instance, within the greater security domain is the accepted practice or professional field, referred to within this study as a cultural domain (Bernard & Ryan, 2010, p. 164) of physical security (Horrocks, 2001, p. 221; Brooks, 2007, p. 5; Talbot & Jakeman, 2009, p. 55; p. 220; ASIS, 2009, p. 3). Physical security is defined by ASIS International as that part of a security program concerned with physical measures designed to safeguard against a security incident using measures as a device, system or practice of a tangible nature to protect people and prevent damage to, loss of, or unauthorised access to protected assets (2009, p. 3).

However, physical security as a cultural paradigm is one of low development when compared to the more traditional academic fields such as physics. For instance, Lodahl and Gordon (1972, p. 68) explain that physics is a highly developed paradigm field, whereas there are many fields which are not and are still in their pre-paradigmatic stage. They explain that the essence of a paradigm or cultural domain relates to the degree of consensus or sharing of beliefs within a field about theory, methodology, techniques and problems. Thus, when compared to well-developed paradigms such as physics, physical security is poorly developed, most likely in its pre-paradigmatic stage. Such maturity will only progress if the important content of the field and its cultural structure is captured. As Lodahl and Gordon (1972, p. 66) point out, the more developed paradigms have more structure and thus more predictability than fields with less developed paradigms.

1.5 The cultural domain of physical security

The combined literature of Clarke (1992, p. 4), The American Institute of Architects (2004, p. 1), Talbot and Jakeman (2009, p. 55), Smith and Brooks (2013) and Bernard

and Ryan (2010, p. 164) lead to the premise that physical security as a professional occupation is a distinct academic paradigm and cultural sub-domain within the broader domain of non-traditional security. In ethnographic vocabulary, cultural knowledge refers to the acquired knowledge that people use to interpret their world (Spradley, 1979, p. 5). Spradley (1979) considers such knowledge to be that which people have learned as members of a specific group (p. 7). Accordingly, the study asserts it is within the specific cultural domain of physical security where security professionals find the knowledge base to analyse, define and solve through economically feasible options and measures those which attain situational and environmental design crime prevention techniques and principles. These techniques combine towards blocking opportunities for particular criminal acts; aspects acknowledged as efficacious and a driver for the self-provision of security for corporations (Prenzler & Sarre, 1998, p. 2).

The objectives of the study therefore sat within an ethnographic architecture, as ethnography according to Spradley (1979, p. 3) is the vocation of describing and analysing a specific culture. Such an analysis was steered towards fusing, through codification, the diverse cultural knowledge of physical security in terms of desired knowledge areas and their supporting content along with its internal structure as an organised knowledge system (body of knowledge) for future physical security professionals and institutions of higher education. Informed by the writings of Spradley (1979) and Bernard and Ryan (2010) this exploration was best achieved through a cultural domain analysis. Spradley (1979, p. 145) explains that a cultural domain's knowledge structure is based on isolating the fundamental units of cultural knowledge (symbols) (p. 142), accordant with a single semantic relationship (p. 145), organised according to concept relationships in terms of similarities and differences (p. 157). Such an articulation highlights internal knowledge structural boundaries, where we discover that some fundamental units belong inside a specific internal boundary due to features of similarity, and that others belong outside because of differences (dissimilarity) (p. 157).

The notion of culture is expanded within the work of Johnson (1995, p. 68) who explains it as "the accumulated store of symbols, ideas, and material products associated with a social system, be it an entire society or a family unit". In other words, it is a shared system of meaning (Spradley, 1979, p. 4). Culture is material and non-material in

nature, where material culture includes everything that is made, fashioned, transformed as part of collective social life, from the preparation of food to the manufacture of steel and computers. Non-material culture includes symbols from words to musical notation- as well as ideas that shape and inform the lives of humans in relation to one another and the social systems to which they participate. The most important of these ideas are attitudes, beliefs, values and norms. This definition is summed up by Malcolmson (2009, p. 361) in reference to security culture as a set of common understandings, expressed in language, or shared patterns of meaning, or shared values and beliefs. As an extension of this literature a cultural domain analysis is expressed as an examination of a domain of interest to elicit it's content (elements) and understand its structure (Bernard & Ryan, 2010, p. 164).

1.6 Underlying theory

The study undertook a cultural domain analysis, denoting an occupational culture as a professional group whose knowledge could be represented through psychological maps revealing both content and structure. The work of Bloom acknowledged psychological structures as a means of knowledge representation and expressed that educational objectives must be related to a psychology of learning. Congruent with the concept of knowledge structure, the use of a psychology of learning enables the capacity to determine the appropriate placement of objectives in a learning sequence. It also helps discover those conditions under which it is best possible to attain identified learning outcomes. The study provides the means of determining the appropriate interrelationships among learning goals (Anderson & Sosniak, 1994, p. 43). A psychology of learning therefore provides the impetus to develop physical security cultural maps, expressed as cultural symbols or heuristics, from a large set of knowledge categories and units, which serve as a guide for acting and interpreting human, and more specifically professional security experience (Spradley, 1979, p.7).

Fittingly, the study drew on cognitive constructivism within the assimilation theory paradigm as its theoretical foundation for exploring a knowledge structure as a formal knowledge system for the domain of physical security. This sought to represent this domain's body of knowledge or formal knowledge system through the use of cultural symbols. Cognition refers to, or means thinking or knowing, with the process of coming

to know something (knowledge) (Tovey & Lawlor, 2004, p. 65). Knowledge is defined as those behaviours and situations that emphasize the remembering, either by recognition or recall, of ideas, materials or phenomena (Anderson & Sosniak, 1994, p. 18). Consequently, since the 1970s, the cognitive perspective has been the strongest influence on learning theory that still endures today (Tovey & Lawlor, 2004, p. 64). In this frame of thinking, learning is explained as the process through which learners construct and integrate new knowledge with existing knowledge within conceptual frameworks to form deep understanding and skilled practice (pp. 59-65).

According to Tynjala (1999, pp. 363-364) constructivism is articulated as a conglomeration of different positions within a theory of knowing with emphasis on how knowledge is built. He claims that accordant with this theoretical frame, knowledge is actively constructed by individuals or cultural communities not just discovered. In addition, constructivism holds that knowledge construction is based on previous knowledge, and that it is constantly evolving over time (Novak, 1993, p. 167); recognising that new ideas are built on the foundation of prior thoughts (Fraser, 1993, p. 16). Within this foundation, Ausubel's (1968) assimilation theory placed central emphasis on cognitive processes involved in knowledge acquisition and the role that explicit concept and propositional frameworks play in knowledge acquisition (Novak, 1993, pp. 171-172). The cognitive perspective of learning views behaviour as being determined by how individuals perceive, structure, interpret and engage with their environment (Tovey & Lawlor, 2004, p. 65). Accordingly, the fundamental principle of constructivism is that learning is a constructive activity that students themselves must undertake (Fosnot, 2005, p. 7), as knowing something includes processes that are internal to the individual. Anderson and Sosniak (1994, p.8), regarding Bloom's views of learning, stated "the more modern view of the learner is that his or her ability is neither permanent nor stable, rather it is highly alterable when proper stimulation and experience are provided".

Piaget (1951) launched the key notion that sets constructivism apart from other theories of cognition, expressing the idea that what humans refer to as knowledge does not and cannot have the purpose of producing representations of an independent reality, but rather is an adaptive function (Fosnot, 2005, p. 3). The concept of adaption stems from biology, and it indicates a particular relationship between living organisms or species

and their environment. Piaget took this notion and deduced that whatever knowledge was, it was not a copy of reality. As such, Piaget considered knowledge to be a mapping of actions and conceptual operations that have proven viable in the knowing subject's experience, rather than a more or less accurate representation of external things, situations and events (p. 4). From this perspective, cognitive structures, i.e. action schemes, concepts, rules, theories, and laws, are evaluated saliently by the criterion of success, and success must ultimately be understood in terms of the organism's efforts to gain, maintain, and extend its internal equilibrium in the face of disturbances (Von Glasersfeld, 1982, p. 6).

According to Von Glasersfeld (1982), Piaget expressed what humans see, hear and feel, that is, their sensory world, as the result of their own perceptual activities and conceiving. Knowledge therefore arises from actions and the agent's reflections on them. According to Fosnot (2005, p. 7) this highlights the point that students perceive their environment in ways that may be different from those intended by educators. The learning environment includes curricula, textbooks, didactic props including computer programs and micro worlds, tasks that have been given, and the teachers themselves. To this point Piaget emphasised that teachers need to construct a hypothetical model of the particular worlds of the students they are facing. Piaget's later works focused towards the mechanisms of learning, that is, the process that enables new constructions, new perspectives to come about (p. 12). Here Ausubel, Novak and Hanesian (1978, pp. 21-27) highlight two clearly distinct forms of learning. That is, the distinction between reception and discovery learning and between rote and meaningful learning.

Supporting the principles of reception learning Ausubel et al.'s (1978) work emphasises that most of the understandings learners acquire both in and out of formal schoolings are presented rather than discovered. In reception learning (rote and meaningful) the entire content to be learned is presented in its final form. Thus, students are not required to engage in independent discovery; learners are only required to internalize and incorporate the material for availability and recall at some later time. In contrast, discovery learning incorporates an essential feature, that the principle content is not presented but must be discovered by the student themselves before it can be meaningfully incorporated into the learner's cognitive structure. Learning by discovery requires a different process from that of reception learning.

For discovery learning, learners must first rearrange information, integrate it with existing cognitive structures and reorganize or transform the integrated combination in such a way that they can generate a desired-end-product or discover a missing means-end relationship. After such learning is complete, the discovered content is then made meaningful in much the same way as presented content is made meaningful in reception learning (Ausubel, et al. 1978, p. 24). Ausubel, et al. (1978, p. 26) argue that discovery learning, or discovery methods of teaching, are not an efficient primary means of transmitting the content of an academic discipline. Rejecting the role of discovery learning Ausubel (1968) argued that reception learning could lead to more meaningful learning; putting forward the idea of an advance organizer which could serve as a cognitive bridge between new knowledge to be learned and existing relevant concepts and propositions in the learner's cognitive structure (Novak, 1993, p. 172).

In essence, cognitive constructivism views humans as developing organisms, not only in the physical and biological sense, but also in the cognitive sense. Piaget proposed and demonstrated through research that the mechanisms promoting change in cognition was the same as that in evolution-equilibrium (Fosnot, 2005, p. 16). This biological landscape characterized by autopoietic systems and dissipative (transforming) structures provide the basis for a psychological theory of learning referred here as constructivism (Fosnot, 2005, p. 27). Autopoietic systems are those systems which reproduce their elements on the basis of their own elements-themselves based on their interactions (Seidl, 2004, p. 2), as cognition is a self-referential, autopoietic process (p. 3). Within this proposition is the viewpoint that human beings have no access to an objective reality, as they are constructing their version of it, while at the same time, transforming it themselves (Von Glasersfeld, 1982, pp. 1-3). But here the focus shifts from the cognising individual, and the culture in which the learning is taking place, or more precisely, to the interplay between them. According to Fosnot (2005, p. 28), we cannot understand an individual's cognitive structure without observing interactions in a context, within a culture.

Yet, according to Fosnot (2005), culture cannot be understood as an isolated entity affecting the structure, because all knowledge within the culture is only-taken-as-shared. The process of construction is adaptive in nature, and requires self-organizing. As stated by Fosnot (2005, pp. 27-28):

> Cultural knowledge that is assumed to be held by members of the culture is dynamically evolving, negotiated interaction of individual interpretations, transformations, and constructions. At best, cultural knowledge can only be assumed, or 'taken-as-shared' by its members. But cultural knowledge is a whole larger than the sum of the individual cognitions. It has a structure of its own which interacts with the individuals who are also constructing it. (Fosnot, 2005, pp. 27-28)

Kelly's (1955) influential work featured such a view. Kelly's (1955, pp. 8-9) early work highlighted that humans look at their world through transparent patterns or templates which they create and then attempt to "fit over the realities of which the world is composed". Acknowledging that the fit is not always great, Kelly asserts that without such patterns the world appears to be such an undifferentiated homogeneity confounding understanding. Kelly called these patterns constructs and considers that even a construct's poor fit is better than nothing at all. Kelly defines such constructs as ways of construing the world. They are what enable humans, and lower animals too, to chart a course of behaviour, explicitly formulated or implicitly acted out, verbally expressed or utterly inarticulate, consistent with other courses of behaviour or inconsistent with them, intellectually reasoned or vegetatively sensed. In general, humans seek to improve their constructs by increasing their repertory, by altering them to provide better fits, and by subsuming them with superordinate constructs or systems (p. 9). According to Kelly (p. 9) these construction systems can be communicated or widely shared.

Kelly's view is supported by the works of Eden (1988) and McLucas (2003) who emphasise the use of cognitive and concept maps to make explicit such constructs or patterns. Fitting with a psychology of learning Eden's (1988, p. 2) work articulated that basic to making sense of our world is the detection of repeated themes and the construal of them using a construct system, where the work of Smith and Brooks (2013, pp. 178-179) states that as a consequence these patterns are viewed as information that can be collated to form knowledge. According to Smith and Brooks (2013, p. 179) the constructs of patterns from associations of information have the potential to represent knowledge. By understanding the patterns of information within a domain of data, knowledge is realized and understood along with its implications; learning occurs by

connecting new information to patterns that we already understand. Furthermore, Eden's work separated the individual construct systems from those of a group (cultural). Eden (1988, p. 7) sees an individual's construct system as a cognitive map, a personal mind map. Construct systems representing the views of several individuals (cultural) are differentiated and labelled concept maps. Concept maps represent shared cognitions, they are an aggregated model of a perceived world.

Fraser's (1993) work referred to group constructs as a shared paradigm, sitting well with this theoretical framework, expressing that groups of individuals can participate in the creation of such a paradigm. Fraser emphasised that such models (concept maps) highlight the structure of a paradigm of enquiry (Fraser, 1993). Fraser also acknowledges that shared paradigms are not static entities, but are in constant states of flux as the individuals who subscribe to them and participate in their creation and maintenance interact with them (pp. 2-4). Consequently, Fraser emphasises the requirement for flexibility in the construction of a shared culture arguing that each individual participating in this paradigm or construct has their own interpretation of it. Therefore, efforts in describing a particular culture must "ride-a-thin-line" between general description of the overarching concepts that make it up, yet allow for a broad range of interpretations of it. According to Fraser, "the term body of knowledge is such a shared paradigm, described by Fraser (1993, p. 25) as the term used to indicate a particular field of study…a shared paradigm".

Current biological models facilitate our human understanding that both the structure of the mind and the knowledge we construct within it, are part of an open system. Knowledge and the mind cannot be separated as one affects the other. Both are being developed as the natural outcomes of the evolution of autopoetic systems characterized by dissipative structures (p. 29). This is a point embraced in the earlier work of Bruner (1977, p. 11) who set forth the premise that learning is enhanced by giving learners an understanding of the fundamental structure of whatever subjects (constructs) we choose to impart…"This is a minimum requirement for using knowledge". Accordingly Bruner (1977, p. 12) explains that the teaching and learning of structure rather than simply mastery of facts and techniques is at the centre of enhanced knowledge transference, especially in terms of explaining the relations between things encountered earlier and later towards establishing new knowledge.

Bruner's writings (1977, p. 12) include the proposition "that all cultures represent the meaning of experience in some way; through symbols, music, myth, story-telling, art, language, explanatory scientific models, and/or mathematical forms". Such a constructive process enables the creation of semiotic spaces where meaning can be negotiated (Bruner, 1977). Constructing symbolic representations empowers humans to go beyond the immediacy of the concrete, to cross cultural barriers, to encounter multiple perspectives that generate new possibilities, to become conscious of our actions in the world in order to gain new knowledge with which to act. This act of representing is what makes us human (Fosnot, 2005, pp. 27-31), where the work of Bloom highlighted that we need a method of ordering phenomena such that the method of ordering reveals significant representations among the phenomena (Anderson & Sosniak, 1994, p. 14).

Thus, within the cognitive constructivist's position, learning is a constructive, building process of meaning-making (constructs or paradigms). This results in reflective abstractions producing symbols within a medium. These symbols then become part of the individual's repertoire of assimilating schemes, which in turn are used when perceiving and further conceiving (Fosnot, 2005, p. 31). As Bruner's work (1977, p. 7) highlighted, grasping the symbolic structure of a subject understands it in a way that permits many other things to be related to it meaningfully. Therefore, many domains are understood through taxonomic structure, where the major task is selecting the appropriate symbols, giving them usable definitions and securing the consensus of the group that is to use them (Anderson & Sosniak, 1994, p. 11).

As such, the broad rules of curriculum, course and program design used to impart and stimulate learning reflect the cognitive perspective in which the learner actively builds knowledge as bricks build a wall (Tovey & Lawlor, 2004, p. 65). Accordant with the proposed outcomes of the study, from a constructivist's approach, learning is considered in essence a process of building knowledge through making connections, or seeing relationships (Fraser, 1993, p. 31). The underlying assumptions within constructivism provided the theoretical underpinning support for bringing together or fusing of a dispersed explicit and implicit knowledge base into a formal professional knowledge system, representing a shared paradigm and labelled a body of knowledge. This system illuminates and explicitly exhibits cultural knowledge areas and their associations with

other knowledge areas, facilitating superior reception learning through the development of cultural symbols within the physical security domain.

The study's research methodology was steered by this broad body of literature, seeing physical security as an emerging professional domain as the shared paradigm of enquiry, referred to as a cultural domain. This literature embedded the view that new knowledge is based on the foundations of previous knowledge. And that in looking to construct such knowledge basic to our making sense of our world is the search for, and detection of repeated themes and the construal of them using a construct system of finite number. Piaget's (1951) work expressed knowledge to be a psychological mapping of actions and conceptual operations that have proven viable in the knowing subject's experience. Eden's (1988) work accepted this view, emphasising people differ from each other in their construction of events as they see or perceive different things in what could be regarded as the same situation by a third person.

Thus the investigation of a shared paradigm (body of knowledge) is guided by a number of key assertions expressed in these works. These include the proposition that (a) man makes sense of his world through the detection of repeated themes, (b) man understands his world (repeated themes) through contrast and similarity, (c) man seeks to explain his world and (d), man seeks to understand the significance of this world by organising concepts hierarchically so that some are superordinate to others. In summary, man seeks to develop meaningful patterns or constructs of his world, as a means of construing the world. Once initially developed man seeks to refine his patterns or constructs to achieve better fits with reality, eventually subsuming subordinate constructs with superordinate constructs or systems. Thus, the primary aim of cognitive (individual) maps is to carefully guide the development of concept (cultural) maps, whereby participants can gently change their mind, and do so creatively and where each person can see their own concepts set in a wider context (Eden, 1988, p. 8), and these become the means of construing the shared paradigm.

This study adopted a constructivist approach through a series of phases which sought to build new knowledge (construct) of physical security's body of knowledge on the basis of previously constructed knowledge (Figure 1.2). Figure 1.3 highlights that consistent with the key assertions expressed in the study's underlying theory each phase of the

study expands the previous phase's outcomes, towards the articulation of a structured knowledge system supported by first iteration learning objectives.

1.7 Research questions and objectives

There are a number of interrelated research objectives (Figure 1.3) assigned to various phases of the study.

1.7.1 Research questions

The study seeks to respond to the research question:

What is a desirable knowledge system (body of knowledge) for physical security professionals as conveyed through the published literature and accessible professionals?

It is premised that this research question can be responded to through the following research sub-questions:

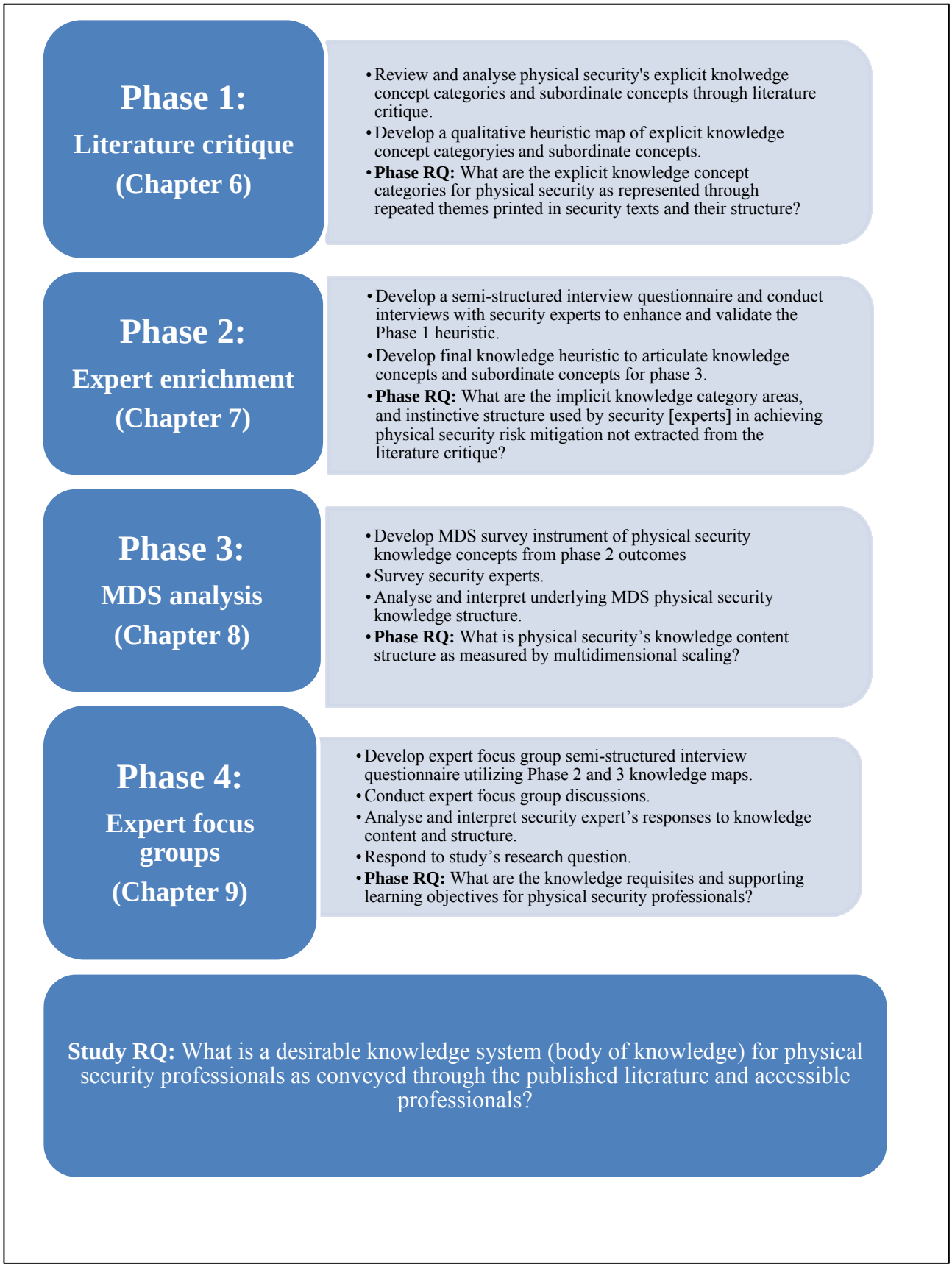
Phase One: What are the explicit knowledge concept categories for physical security as represented through repeated themes printed in security texts and their structure?

Phase Two: What are the implicit knowledge categories, and instinctive structure used by security [experts] in achieving physical security risk mitigation not extracted from the literature critique?

Phase Three: What is physical security's macro knowledge content structure as measured by multidimensional scaling?

Phase Four: Based on the extracted knowledge system, what are the knowledge requisites and supporting learning objectives for physical security professionals?

Figure 1.3 Study phases flow chart



1.8 Reflection

The reviewed literature illustrates that security, as a professional occupational category, is a broad and poorly defined domain. Nevertheless, considerable discourse is progressing towards identifying domain structure and vocational seating within this occupational mosaic. The chapter conceptualized the profession of security as a broad cultural domain where the very notion of security forms the cover term for the domain. This cover term (security) is supported by additional terms, which include categories of knowledge (constructs) accordant with some cultural boundary, and that are all semantically related. From the background literature it is inferred that physical security in terms of implementing situational crime prevention and environmental design measures to reduce the opportunity for, and fear of crime and disorder in society and for governments and organisations is an included term (knowledge category) of security.

Nevertheless, the cultural domain of physical security in the professional strata of society is poorly conceived. The domain (included term) is saliently understood across broader society as a collection of occupational categories (Table 1.1) associated with discrete areas of applied expertise. However, the concept of the security professional, and more specifically the physical security professional, radiates as someone providing advice at a more sophisticated level, accordant with notions of professional strata. Their roles are arguably more focused towards coordinating the combined attributes of the occupational categories (Figure 1.1) to achieve a broader more significant product in relation to an identified professional problem. As Fennelly's (2013) work highlight, physical security has become increasingly complex, where often many complex, interrelated controls are integrated to protect in a given security context.

However, it is expressed that the very notion of the security professional and its bounded physical security professional will remain obscure to most outside of the domain, and perhaps many within, unless an ethnographic analysis of this cultural domain is undertaken. Such an analysis must clarify the sub set borders in professional practice, identify the units of knowledge for the category of physical security professional, and provide their cultural structure. This analysis would lead to an evaluation of what this structure means for future physical security professionals in terms of knowledge and educational requirements, and how these requirements can be

needs met through the higher education fraternity. The needs required for professional practice were implied to be a psychological structure of superordinate and subordinate knowledge concepts, theories and principles semantically related to the domain's cover term security.

Subsequently, the chapter drew on cognitive constructivism as its theoretical foundation, based on a theory of learning where knowledge is constructed based on previous knowledge not discovered. In this frame of thinking learners acquire new knowledge based on the foundations of their previous knowledge; where from a constructivist's approach learning is considered in essence a process of making connections, or seeing relationships. The Interim Australian Security Professionals Task Force (2008) put forward the idea that an educational stratum could exist for security, which links educational attainment to professional employment. As such, the study asserts that this can only be achieved through a thorough ethnographic investigation in the form of a cultural domain analysis. Such an analysis will see the research enquiry driven by a clear set of research questions that are supported by a set of research objectives towards elucidating the knowledge content and structure for this cultural domain.

1.9 Conclusion

This chapter presented the background discussion for the study, highlighting the current occupational diversity within security's greater domain space, and definitional concerns stemming from this diversity. Section 1.2 highlighted the background debate regarding what constitutes the modern day security professional. Then Section 1.3 conveyed the significance of the study accordant with this discussion, where it was expressed that unless academia investigates the academic basis for relevant industry qualifications, the security industry cannot progress towards one with professional designation. Security's professional discourse was extended in Section 1.4, discussing the Australian security industry within the context of the study. This discourse highlighted the occupational mosaic of the physical security domain within Australia through Table 1.1 and Figure 1.1. In this section it was emphasised that in Australia, as with global trends, the use of self-reliant security is a growing leaning, where it is acknowledge that security is a dynamic and evolving sector within the Australian economy. Section 1.5 presented

limitations in the current discourse debating what determines a security professional within the Australian context and embedded physical security as separate occupational domain within the broader cultural domain of security (Section 1.5).

Within this chapter Section 1.6 presented constructivism as a theoretical foundation supporting the assembling of a body of knowledge for physical security professionals, facilitating a response to the study's research questions based on the concept of knowledge building. This discussion was supported in Section 1.7 which stated the study's research objectives, supported by individual Phase outcomes and overarching research questions (Section 1.7.1). The chapter also presented a flowchart showing individual phases of the study and their interrelationships in responding to the study's overarching research question. Section 1.8 summarised the chapter, reflecting on the reviewed literature in preparation for the literature informing the study presented in chapters 2 and 3.

The combined literature indicated that a thorough review of the term security as the domains cover term is essential for understanding physical security as an additional term (sub domain). This literature also highlights that a clear understanding of what a professional is in terms of occupation, their knowledge constructs and educational objectives and requirements is essential for guiding the study's research path. Finally it is acknowledged that a review of professional knowledge mapping is also required to ensure the validity of the study and its adopted methodology for elucidating the knowledge system or body of knowledge for physical security professionals and their educational objectives.

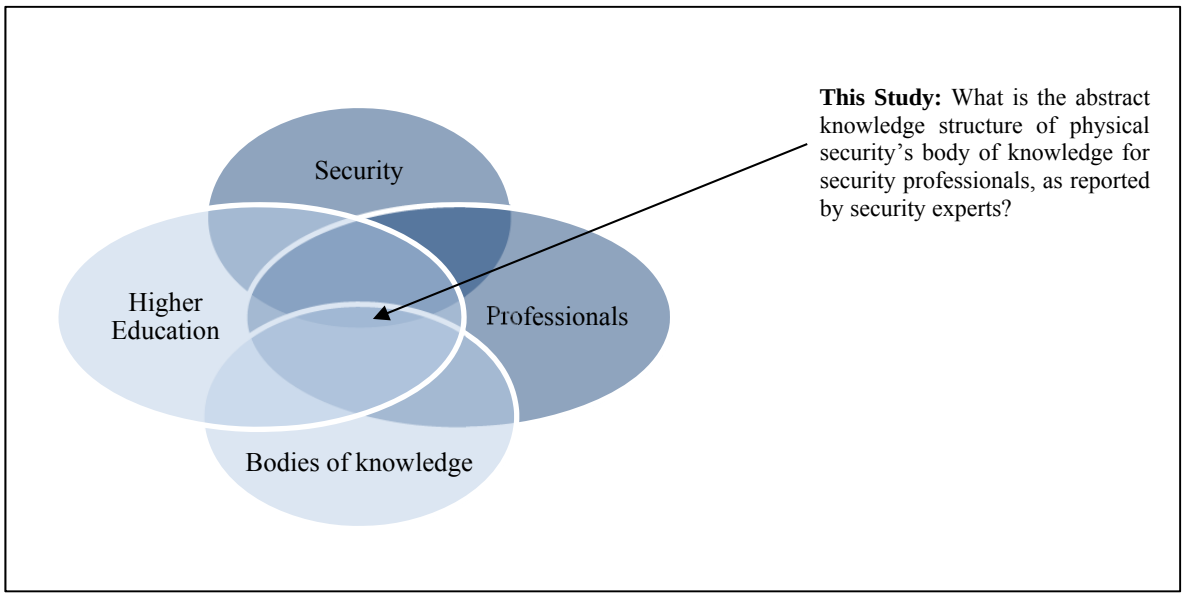
Chapter 2: Security and professionalism literature informing the study

2.1 Introduction

The very notion of security underpins the conception of the security professional and its emerging occupational embodiment. However, the embedded depth and breadth of security within modern society confuses understanding of who or what constitutes a contemporary security professional, their roles and knowledge requisites along with jurisdictional boundary. Chapters Two and Three therefore present the foundational literature informing the development of a cultural body of knowledge for physical security professionals. This understanding was achieved utilizing a conceptual literature review, which according to Stake (2010, pp. 109-111) highlights the broad and complex works from multiple disciplinary areas that combine to extend the comprehension of an area of interest. The conceptual literature review is represented through Figure 2.1, which includes the conceptual basis for the security professional, the theories and approaches underpinning professionalism and their underpinning body of knowledge and its relations to higher education.

This chapter is divided into distinct literature discourses, which contribute to the seating of the study. Security's conceptual denotation is established in Section 2.2, which articulates a conception of security as a broad domain cover term. This articulation is followed by Section 2.3, which conceptualizes the term professional, highlighting designation, as professional status is a social acknowledgement from the broader community rather than by individual occupational domains. The social designation view is reinforced by cognitive dimensions of professional knowledge, discussed in Section 2.4. Then, individual professional expertise is explained in Section 2.5, which is supported by knowledge-based views of domain expertise acquisition in Section 2.6. This literature is enhanced through a discussion of the professionalisation process in Section 2.7. The chapter then concludes with Section 2.8.

Figure 2.1 Research themes of the literature review



2.2 The concept of security

Cultural domains and their supporting taxonomies are based on a single semantic relationship represented through a cover term (Spradley, 1979, p. 145); which for this study is the superordinate axiom: security. As such, informing the study is the acknowledgement that security as an axiomatic construct towards the preservation of life, maintaining rightful custody of possessions (Manunta, 1997, p. 11) and more broadly protecting interests is one of ancient need (Underwood, 1984, p. 3); considered "as old as life itself" (Manunta, 1997, p. 20). Consequently, it is well recognised that humans pursue and achieve a state of well-being through their actions, such as banding together into groups for mutual protection or through diplomacy to avert wars (The American Institute of Architects, 2004, p. 1). Historically under this cover term humans have actively pursued a state of well-being through specific activities targeted towards protecting from the malicious actions of others (Somerson, 2009, p. 51).

Post-modern conceptions and pursuits of security have their roots embedded in ancient times. For instance, Neanderthal man pursued protection by grouping in tribes and altering entrances to their caves utilizing rocks to shield themselves and their possessions from attack (Schnabolk, 1983, p. 2). The historical walls of ancient cities such as Troy, Jerusalem and Jericho show that as humans evolved they pursued protection from more organised foe through more advanced social networks and engineered means (The American Institute of Architects, 2004, p. 4). Such undertakings

have interrelated social and physical means for protection, meaning a state of security also infers a social relationship (Roe, 2008, p. 778). As Clements (1990, p. 4) points out, security flows from social processes, which reduce risks, enhance normality, predictability and mutual reassurance. Accordingly, the cover term security has a long and functional history with mankind, as it is this historical pursuit that is pan-culturally termed security, or a state of being secure.

Nevertheless, regardless of its historical roots, security has and continues to embody many definitions and usages (Griffith, 1997, p. 4). Accordingly, security as a contemporary cover term is considered so multidimensional such that no consensual definition exists (Manunta, 1997, p. 12; Smith & Brooks, 2013, p. 2). As Neocleous (2007, p. 350) points out, today the need for security is so amorphous and ambiguous its application is almost limitless. In this current state of definitional opacity various authors including Baldwin who contends that the word security has become simply a used and abused term. According to this discourse the term security has been devolved into an issue or banner to be flown, or a general label to be applied depending on agendas (Baldwin, 1997, p. 9). Such agendas cloud the very notion of security.

The work of Inglehart and Norris (2012, p. 79) avowed that if everything becomes a matter of security such as: food security, environmental security, political security to economic security, along with many other adjective categories which precede its namesake, then the word loses its core meaning. Except, security is, as it has always been, a significantly important human concept, as the alternative of insecurity is not an option in any stable society (Baldwin, 1997, p. 9; Corkill & Coole, 2013, p. 142). This literature presents a fundamental question for the study: if the very concept of security cannot be defined, then how can we define a security professional and identify their knowledge base?

2.2.1 Security as a means of survival

The writings of Baldwin (1997, p. 9) and Caballero-Anthony (2008, p. 510) coupled with a diverse breadth of contextual labels elucidate security in contemporary times to be a vast and perhaps vague concept contested in varying paradigms. As Roe (2008, p. 780) states:

> If we widen the definition of health to encompass the welfare of the individual in all its dimensions…we weaken our ability to allocate resources to a coherent and manageable health policy. Similarly, an exhaustive concept of security embracing all that contributes to human well-being, as well as perceived threats to it, would be too comprehensive and also useless. (Roe, 2008, p. 780)

Therefore security as a domain must have societal boundaries, where concerns can be rightly included or excluded according to some criteria; conceivably their similarity or dissimilarity to what is denoted by the cover term security. Consequently, to begin the study it is necessary to communicate what is meant by society through this superordinate axiom, Security. Therefore, the study draws on the astuteness of Socrates who articulated that for any true enquiry there must be some singular (shared) description that covers all of its cases. Socrates stressed that many varieties of an enquiry cannot be what the enquiry itself is; rather their shared name must denote something the same for them all, and it is this, which needs defining (Day, 1994, p. 1). Socrates' view of virtue highlights this point, as he premised that:

> Many varieties of virtue cannot be what virtue itself is, their shared name 'virtue' must denote something the same for them all, and it is this which needs defining…presumably it would be right to focus on this in one's answer, and show the questioner what virtue is. (Day, 1994, pp. 1-37)

Socrates did not seek an implicit meaning through countless examples, but sought what the thing really is - the essence of what is denoted by the word (Day, 1994, p. 84). If Socrates' insight is accepted, than the many contexts applied to the term security do not denote what security is, as its diversity must have a shared meaning, and it is security's shared meaning which grounds the concept and its practice domains, and therefore this study. Subsequently, any conceptual analysis of security as a domain cover term must be considered in the broadest possible sense. A view supported in the work of Baldwin (1997, p. 8) who emphasised that understanding the concept of security precedes the conditions under which it can be attained.

Baldwin (1997, p. 8) pronounced that the concept of security is different from the functional means under which it is pursued and realized. Here it is contended that concept definition embedded into contextualization facilitates tailored attainment. Thus, security in modern times can debatably be understood through an analysis of its origins (Burstein, 1996), along with its contemporary connotations, as security has always been, and will continue to be an important human requisite (Misiuk, 2011, p. 255). The influential work of Mill (1910) and Maslow (1970) recognised this point. Mill (1910, p. 50) noted that security is the most vital of all human interests after physical nutrition, expressing that all other earthly benefits are needed by one person, not needed by another, and many of them can, if necessary, be "gleefully forgone", or replaced by something else; but security no human being can possibly do without, "on it we depend for all our immunity to evil" (p. 50). Maslow's work supported this view through his renowned hierarchy of needs, stressing that at the most basic level humans require physiological needs to be met to ensure their survival. Then it is acknowledged of the necessity to protect these needs (Maslow, 1970, pp. 35-46; Paris, 2001, p. 102) before higher level needs can be pursued and maintained.

These combined works emphasise security as a vital aspect of human life (Mill, 1910, p. 50; Maslow, 1970, pp. 35-46; Manunta, 1997, p. 11). As such, Maslow's (1970, pp. 35-46) hierarchy of needs has been entwined with numerous conceptualizations of security. Such views arguably fall within sociology's conflict perspective. Conflict theory predicates that social life is shaped by groups and individuals who struggle or compete with one another over scarce resources, and that such competition leads to conflict (Johnson, 1995, p. 52) and consequently insecurity. Subsequently, once these physiological needs are met, safety and security needs are crucial before other higher human developmental needs can be pursued (Maslow, 1970, pp. 35-46). This hierarchy provides a lens presenting in a protective sense safety, and more contextually security as a significant human concern.

However, Maslow's writings highlight an embedded overlap between safety and security, except in modern times these terms have become very distinct occupational concepts. Safety in contemporary industrial language focuses on hazards or accident management (Somerson, 2009. p. 51), whereas security's focus is towards managing malicious centred human acts articulated as threats (Garcia, 2001, p. 2) rooted in

conceptions of risk. As the American Institute of Architects (2004, p. 22) express, safety threats arise from natural or accidental conditions. In contrast, security threats result from actions planned and carried out by people where "security threats are intentional and originate in human actions". Such a view resonates across the security literature. For instance, McSweeney (1999) highlights that those threats grounded in the purposive behaviour of other actors, social-threats, are distinguishable in terms of the policy required to address them from those which arise from the chance occurrences of the natural order, they require different measures.

Thus, a theory of security if it is to be appropriately bounded to facilitate effective mitigation must arguably be framed within a purposive behaviour paradigm. Accordingly, any theory of security in an adversarial sense, must be a social theory, as social relates to "(1) living or preferring to live in a community rather than alone, (2) relating to human society and organization, (3) behaviour and interaction of persons" (Collins Dictionary, p. 805); and without other humans to threaten, there is no need for security, regardless of context. Within a human centric paradigm security must consider that behaviour is planned or spontaneous as a result of cognitive processing factors. This accounts for a separation of planned and opportunistic threat typologies which both manifest security related consequences. Accordingly, a security threat or risk is someone or something that intends to, or could, cause harm (Smith & Brooks, 2013, pp. 8-9) to someone, or something valued (Wolfers, 1952), be it planned or opportunistic. In this sense, threat drives risk (Coole & Brooks, 2011, p. 54), where a security risk is any assessed and evaluated threat event that could compromise the well-being of people or the integrity of interests or assets designated for protection; the central term being risk (Talbot & Jakeman, 2009, p. 7).

Recognising this occupational dissection, the work of Talbot and Jakeman (2009) comprehend the concept of security to be a state of being protected (secure) in response to conditions of risk. However, security risks are pervasive, where nowadays both the functional embodiment and academic study of security is entrenched into most aspects of daily life (Corkill & Coole, 2013, p. 142), resulting in a diverse and emerging domain (Smith & Brooks, 2013, p. 2). Plus, while the concept of security has an embedded history with human kind, as both a professional and academic field security is young, lacking singular definition (Manunta, 1997, p. 12; Smith & Brooks, 2013, p. 2), or in

the words of Socrates, ‘what it is’. For this reason, security’s contemporary conceptual discourse embodies many understandings, contexts and definition, clouding singular understanding of the cover term security.

Such diverse conceptions lead to security’s reference as multidimensional in nature and ubiquitous (Brooks, 2010, p. 225) to the point of impeding clarity (Manunta, 1997, p. 12; Smith & Brooks, 2013), except within applied contexts (Brooks, 2007), thus, arriving back at Socrates’ contention. Nevertheless, it is broadly recognised that security as a concept includes both philosophical and operational (functional) facets (Baldwin, 1997; Manunta, 1997), which have followed a pattern of communal evolution within that of social organisation, from individual-family to band, tribe, chiefdom and state (Manunta, 1997, p. 22), and arguably these facets can be analysed to articulate what security is.

2.2.2 The depth and breadth of the security domain

Today, both philosophically and functionally, security is considered at a macro level of analysis, from an international perspective with concerns towards safeguarding the sovereignty and territorial integrity against threats to a nation itself (traditional security) (Wolfers, 1952; Ullman, 1983; Rothschild, 1995; Baldwin, 1997); through to a micro perspective, with an emphasis on individual citizenry protection (non-traditional security) (Rothschild, 1995; Cabellero-Anthony, 2008; Pion-Berlin, 2010), and capturing every other malevolent risk concern in between. Consequently, within security’s multidimensional scope lies a broad range and sizable number of contexts and definitions that hinder monolithic classification and therefore obscuring the denotation of what security is.

Griffith (1997) notes that many usages or definitions of security are based on traditional realism. The realist approach focuses on the state as the unit of analysis and stresses the competitive character of relations among states (p. 4). The traditional paradigm of security has therefore viewed security risks at a macro level, as malevolent threats associated with the conflict of war between states over resources and political agendas, embodied within the euphemism of national security (Reveron, 2011, p. 2). This domain of security views states as national actors, rationally pursuing their interests, focuses

saliently on external threats, and sees military and economic power capabilities as critical tools in achieving security (Griffith, 1997, p. 4). In this paradigm it is acknowledged that all nations have a right to defend themselves from threats (United Nations., 1986, p. 1), where Wolfers (1952, p. 482) expresses that national interest has become synonymous with the formula of national security. Within his understanding, Wolfers' (1952, p. 485) seminal work saw security as a value, and defined security accordingly as "the absence of threats to acquired values, in an objective sense, and in a subjective sense, as the absence of fear that such acquired values will be attacked".

According to Wolfers (1952, p. 484), values represent characteristics such as national independence, territorial integrity, power, wealth, national character, tradition, individual liberty or preferences, and considered security to encompass both a physical and psychological state of being. Congruent with this body of work, Griffith (1997, p. 5) saw security as the protection and preservation of a people's freedom from external military attack and coercion, from internal subversion, and from the erosion of cherished political, economic and social values. Accordingly, Wolfers' (1952, p. 500) security contention is that countries must hierarchically choose the values that deserve protection.

Such literature highlights that values or interests may be regarded as higher or lower order. For example, in more recent times The United Nations broadened this archetype, establishing the theory of international security, a macro theory of security articulated as the sum of security of each state member of the international community. This in the words of Wolfers (1952, p. 482) would include the protection of values for all of mankind, especially when facing present-day security risks such as nuclear weapons, which pose a global threat (United Nations, 1986, pp. 2-8). In this contextual environment, the United Nations (1986, p. 9) contended that international security must sit within a commitment towards joint survival rather than a threat of mutual destruction. Such a characterisation reinstates the concept of collective security, where as with Neanderthal man, security is pursued collectively, as a community. However, this communal pursuit is broader through the uniting of the Nation state's interests based on a global commitment to international peace and security.

Nevertheless, security is more than a macro state condition, as nation states cannot forget the legitimate concerns of ordinary people who seek solace in their daily lives (Inglehart & Norris, 2011, p. 74). In today's global community, security is considered an inalienable right for every human being; all people have the right to life, liberty and security of the person (Article 3; The United Nations Universal Declaration of Human Rights). As such, many security scholars, supported by international organisations (United Nations Development Programme) along with National governments advocate towards a broader thematic category labelled human security (Nef, 1999, p. 25; Paris, 2001; Roland, 2001, pp. 89-91; Inglehart & Norris, 2011, p. 74). This purportedly embodies those security-associated concerns that threaten human survival, conditions of daily life and the individual's dignity. This perspective is underpinned by the contention that such a broader linguistic embodiment of security dissolves previous boundaries and existing paradigms to link multiple risks and threats for enhanced understanding. The concept of human security still embraces sovereignty threats, but also includes a much broader range of societal concerns (Inglehart & Norris, 2011, pp. 71-74).

The work of Nef (1999, p. 25) expressed "human security's incarnation to comprise five component groupings, including: (1) environmental, personal and physical security concerns, (2) economic security, (3) social security, (4) political security, and (5) cultural security". Yet in contrast, Inglehart and Norris (2011, p. 74) proposed seven major component groupings for human security, including economic security, food security, health security, environment security, personal security, communal security, and political security. Paris (2001, p. 91) highlights that such articulations represent more a laundry list approach, where again the notion of a rallying cry appears in the literature. Existing definitions of Human Security are expansive and vague, over inclusive, where everything from physical security to psychological security is encompassed under the one neologism (Paris (2001, pp. 87-91). For example, the work of Blatz (1967) expressed the concept of human security to be related to children's psychological development within the child study domain.

Accordingly, the human security paradigm's discourse is embedded in disparaging views without consensual agreement of themes or monolithic delineation. As Paris (2001) states:

> Human security can be said to have two main aspects. It means, first, safety from such chronic threats as hunger, disease and repression. And second, it means protection from sudden and hurtful disruptions in the patterns of daily life-whether in homes, in jobs or in communities…Virtually any kind of unexpected or irregular discomfort could conceivably constitute a threat to one's human security. (Paris, 2001, p. 89)

Most formulations of human security emphasise the welfare of ordinary people (Paris, 2001), and could be re-expressed as values accordant with the words of Wolfers (1952, p. 485). For example, Griffith (1997, p. 4) premised that political security pertains to the stability of nations and the ideological and organizational elements that facilitate their maintenance. In contrast, economic security is concerned with the monetary equilibrium of states such as the availability of, and access to economic capabilities. On the contrary, environmental security pertains to the maintenance of the eco system, or at least to the prevention of its deterioration. All contextual security examples represent conditions that, if altered to the negative, affect the welfare of ordinary people.

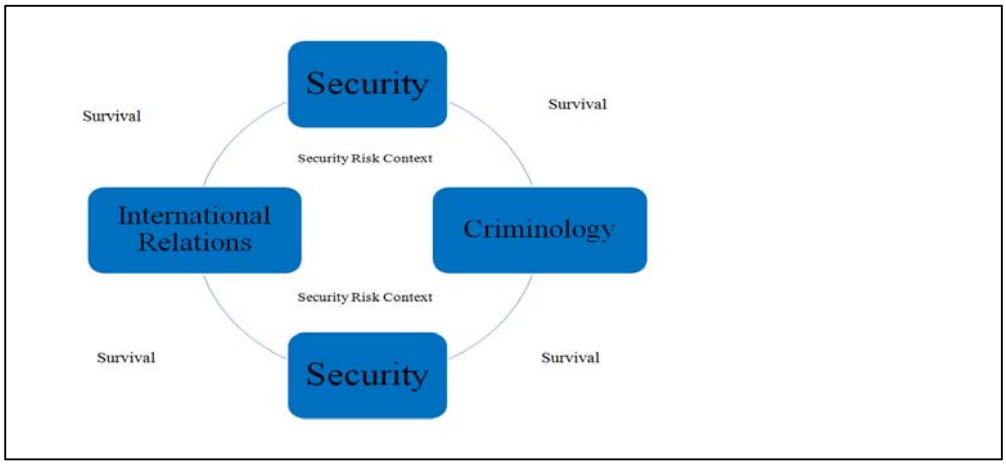
Nevertheless, the concept of human security remains theoretically contested (Inglehart & Norris, 2011, pp. 79), as attention must also be paid to further threats that transcend national boundaries, which directly affect persons, and also threaten to erode national cohesion, ultimately degrading domestic well-being. These threats include for example, drug trafficking, transnational organised crime, nuclear smuggling, refugee movement, uncontrolled and illegal immigration, environmental risks and international terrorism, all of which capture concerns of human existence (Edgar & Ifantis, 2007, p. 452).

Security's focus throughout this literature is illuminated as the means or measures towards maintaining survival and conditions of human existence as a collective concern in the face of a decisive threat. Such thoughts were earlier voiced by Baldwin (1997, p. 13) who altered Wolfers' phraseology to define security as "a low probability of damage to acquired values" to consider impacts of natural events as well as harms from conflict. As Baldwin highlights, in ordinary language references to epidemics, floods, earthquakes, or droughts as threats to acquired values can be found. Thus, security is valued not only by states and other actors, but individuals and families (Baldwin, 1997, p. 18).

Accordingly, the writings of Colak and Pearce (2009, p. 13) re-acknowledge that states within contemporary society must protect communities and individuals from a wider set of risks than traditional sovereignty threats. States must, accordant with the values approach, focus towards conditions for well-being and social justice while being respectful of democratic values and human rights, along with accountability to their citizens. Such an extension is symptomatic of security's emergence as both a condition of States themselves (sovereignty), and the conditions for individuals within them (society), that is, a macro-meso-micro relationship. These writings again express the existence of threats which pose a risk outside of the military paradigm, but which still challenge the survival and well-being of States and their peoples (Caballero-Anthony, 2008, p. 510) that are embedded with referents of security. As the writings of Maslow (1970) highlighted, if conditions of security are eroded, rapid reversions in his hierarchy of needs occurs until such a state can be restored.

Thus, security is not just about the State as an entity, but also people themselves, at the societal and individual levels (Caballero-Anthony, 2008, p. 510). Therefore, security is seen as a pursuit in the traditional sense (traditional security), through the politics and international relations domain. However, the shift in conceptualizations of security in the 21st century has also thrust security to forefront of the criminological (Zender, 2009), sociological-societal (Neocleous, 2007) and legal (Beccaria, 1775) agendas as well. As Neocleous (2007, p. 346) highlights, security is implied to be a public good. Where now in the personal sense security has been saliently embodied within the domain of criminology (non-traditional), constituted within a state-society-individual relationship (Figure 2.2) (Rothschild, 1995, p. 61). It is within this relationship that Cotterrell (1984, p. 5) affirms the concept of security to be one relating to a state of regulation of behaviours, achieved functionally through the provision of norms and laws.

Figure 2.2 Security as a dual domain embodiment



Cotterrell's (1984) views are supported by the functions of the first recorded body of law in the code of Hammurabi, established in approximately 1700 B.C. The Code sought to regulate societal concerns including trade, commerce, agriculture and the early professions (Schnabolk, 1983, p. 2). From their early origins the charters of laws relating to the regulation of society evolved over time, and the pursuit of protection under the banner of security was part of this evolution. For example, in England an historical legal prescription under the banner of security includes the formal requirement to clear brushwood and other concealments within 200 feet from the side of the King's road, to protect travellers against attacks from robbers, thus providing security (Fischer & Green, 2004, p. 22).

Consistent with this view, Cotterrell's (1984) contention was that the law is the practical craft of systematic control of social relations and institutions; it is the practical craft of government towards a state of security. The earlier writings of Beccaria (1704, p. 6) highlighted this very point, stating "society's laws are the conditions under which men, naturally independent, united themselves in society". Through laws individual liberties were sacrificed towards the pursuit of a common good of peace and security (Beccaria, 1775, p. 6). Here the work of Misiuk (2011, p. 255) articulated that a State predominately serves to fulfil psychological needs, inter alia, in the field of feeling secure; and that the vast majority of the State's organisation through its institutions and legal regulations concern the very concept of security.

The communal-legal conceptualization of security encompasses the idea that the State formally provides security in return for individuals surrendering a portion of their liberty. This occurs through an embedded contract between the public and State as a civil right of personal security. Such rights include, for example, freedom from assault, rape and coercion of various types, where the corresponding duties on the part of fellow citizens, government and its proxies, and social agencies are to abstain from deviant acts (Yanay, 2006, pp. 511-513). Within this paradigm security becomes synonymous with crime prevention, where Makinda (1998, p. 282) defines security as a concept concomitant to "the preservation of the norms, rules, institutions and values of society", perspicuous through laws. Such writings re-emphasise the notion that man pursues security communally, through dedicated actions. Furthermore, these actions seek to control the actions of others, which in this notion is through the provision of society's laws and norms, both globally and locally regulating against deviance to provide a state of being and feeling secure.

Consistent with this proposition, Rothschild (1995, p. 61) explains that society's understandings of security in the personal sense reflected early political ideas and stemmed from the Latin word securitas referred, in its primary classical use, to "a condition of individuals, of a particular inner sort; securitas denotes composer, tranquillity of spirit, freedom from care, the objective of supreme desire". Rothschild (1995, p. 61) expresses that one of the principle synonyms for securitas, in the Lexicon Taciteum, is Sicherheitsgefuhl: the feeling of being secure. In this paradigm, Burstein's (1996, p. 1) writings acknowledge that the entitlement to protect one's self and property against attack is a notion of ancient origins, where the primary responsibility for protecting against harms through deviant means or otherwise rests with its owner.

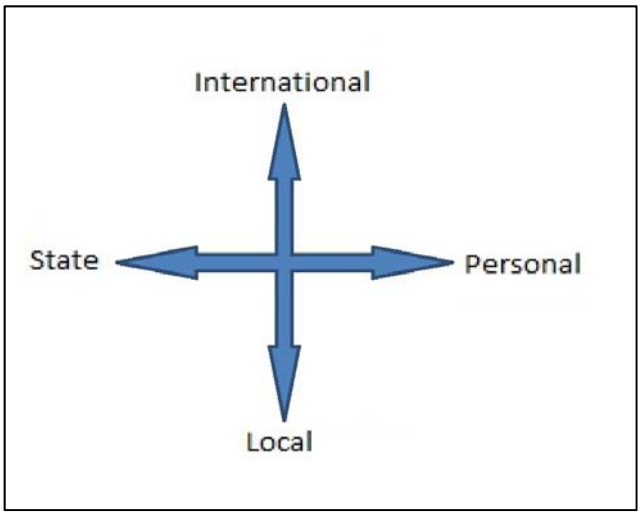
Such a notion was articulated in an organisational sphere within the early industrial writings of Fayol (1949), who recognised this responsibility for successful business operations, identifying the protection of assets and personnel as one of the fundamental functions of industrial undertakings. Fayol (1984, p. 9) defined security as to safeguard properties and persons against theft, fire and flood, to ward off strikes and felonies and broadly all social disturbances liable to endanger the progress and even the life of the business. Fayol (1984, p. 11) stated that those responsible for security protect the firm against all forms of threat to its assets and personnel, underscored through risk

management. The background to such a view stemmed from the Greek city-states, which were the first to establish formal domestic security to protect life and property through the Praetorian Guard, established by Caesar Augustus, Emperor of Rome at the time of Christ, to protect him and the palace, who eventually evolved into the Urban Cohorts to also protect the city (Schabolk, 1983, p. 2).

Yet despite both a clear contextual and historical emphasis within this sphere, security incorporates a vast array of varying definitions. For instance, Underwood (1984, p. x) defined security as "confidence in the retention of belongings, confidence in personal safety". Alternatively, O'Block, Donnermeyer and Doeren (1991, p. 7) define security as "freedom from fear of crime and the actual danger of being the victim of crime". Such views are supported in principle through Craighead's (2003, p. 21) definition, "free from danger, or safe". However, Fischer and Green (2004, p. 21) expanded these formations, stating that security in broader terms implies "a stable relatively predictable environment in which individuals or groups may pursue its ends without disruption or harm and without fear of disturbance or injury". O'Shea and Awwad-Rafferty (2009, p. 7) also consider the notion of security along psychological and physical states, defining security as "free from risks of loss, and free from danger, fear and anxiety", emphasising both feelings (psychological) and a physical assurance.

Such literature are consistent with the writings of Brooks (2010, p. 225) in that security is a multidimensional concept. Derived from the writings of Corkill and Coole (2013, p. 144) this view is graphically expressed through an intersecting two-dimensional diagram (Figure 2.3) that captures a macro-meso-micro representation of such an embodiment. This represents security as a concept along intersecting continuums from a global-international theme to a local national concern, intersecting across another continuum from a state to an individual-micro focus. It is argued that this graphical representation better captures the breadth of security's occupational and academic dimensionality.

Figure 2.3 Two intersecting continuums of security's multidimensional embodiment (Derived from Corkill & Coole, 2013, p. 144)



Nevertheless, Figure 2.3 only captures security's dimensionality, rather than monolithically articulates the cover term security. The Manunta (1997, p. 19) centric paradigm considered security in its broadest sense (Philosophically) to be an attempt to reach and maintain a state of, absence or freedom from danger and worry, a point expressed by Corkill and Coole (2013, p. 147) in their phrase "freedom of action", or "freedom to act without fear of threat". On the other hand, in its operational or functional sense, Manunta (1997, p. 19) considered security as a "set of functions and activities aimed at preventing unacceptable losses and damages to those tangible and intangible assets considered worthy of protection". In these words security is the pursuit of a desired state, to protect from threat, for as Manunta contends, "if there is no threat, there is no need for security".

The reviewed literature highlights that all security perspectives arguably embody overarching philosophical and functional aspects to contextually provide a desired state of affairs. Within this view it is considered by Baldwin that regardless of where security sits dimensionally, they are all interrelated stating "security at the individual level is related to security at the level of the state and the international system". A viewpoint also accentuated in the work of Paris (2001). In pursuit of a contextually secure state the standard rational from within the international perspective (traditional domain) is that security is about power (Stone, 2009, p. 2). Yet the emerging theme within the

criminological perspective (non-traditional domain) is that security is about control, real and perceived.

2.2.3 Denoting what is meant by the word security

The work of Corkill and Coole (2013, p. 143) bridge the traditional and non-traditional security domains views together, arguing power is a means of pursuing control, a view arguably implied in the earlier writings of Wolfers (1952, p. 485) who stated, "power is the ability to control the actions of others". As such, Corkill and Coole (2013, p. 143) affirm that the term security is linguistically a lulling term for the word control, and it is mechanisms of control, which brings about a contextual state of security, or in the words of Fischer, Halibozek and Green (2008, p. 31), "a stable and predictable environment".

In addition, security is not a static concept, as humans have continually been developing the means to protect themselves and their possessions from the dawn of time, constantly devising and refining protective systems (Schnabolk, 1983, p. 2). According to the American Institute of Architects (2004, p.183) "Security can only be achieved through constant change, through discarding old ideas that have outlived their usefulness and adapting others to current facts".

Such combined actions influence or control potential threat actor's behaviour to achieve what Coole (2010) referred to as a steady state condition, or again, a predictable environment (Fischer, Halibozek & Green, 2008, p. 21). Such a viewpoint is acknowledged in the writings of Borodzicz and Gibson (2006, p. 182), and Fischer, Halibozek and Green (2008, p. 31) articulating that security is a dynamic process, responsive in time and place. Security approaches are gradually altered throughout history "as a response to, and reflection of, a changing society". Brooks (2010) acknowledges this theme, describing security as both changeable in nature and function. Such a broad discourse is captured in the writings of Stone (2009):

> Security is taken to be the pursuit of freedom from threat and the ability of states and societies to maintain their independent identity, and their functional integrity against forces of change, which they see as hostile. The bottom line, security is about survival, but it also reasonably includes a

> substantial range of concerns about conditions of existence. (Stone, 2009, p. 1).

Security, along with safety, is among the most basic and central human needs and rights (O'Shea & Awwad-Rafferty, 2009, p. xv). Nowadays, security is still about survival, conditions of existence along with the retention of belongings, but at the international, national, state or regional, organisational and personal levels. In these societal strata, the depth and breadth of the contemporary security domain is represented through thematic categories, neologisms or euphemisms accordant with the adjectives that precede its namesake. For example, national security, human security, energy security, water security, food security, border security, aviation security, maritime security, organisational security, cyber security, or information security (Corkill & Coole, 2013, pp. 145-146). Therefore, security is more recognised by its context (Baldwin, 1997). But again, as Socrates pointed out, many categories of security do not denote what security is. It can be argued that all adjective categories embody legitimate concerns that threaten survival or conditions of daily life. According to Borodzicz and Gibson (2006, pp. 181-182) a common thread within the security discourse is the desire on part of all to protect against malicious human intervention in the form of perceived risks and perpetrated consequences using a variety of countermeasures.

As such, the examined literature highlights that, as an axiomatic construct, security remains a broad term, encapsulated in various linguistic forms, where a singular conjugal definition is unlikely in the near future. Yet the cultural domain taxonomy for physical security professionals is based on the single semantic relationship with the axiom security; where semantic is defined as "(1), relating to the meaning of different words or symbols, (2), of or relating to semantics; where semantics is defined as (1), the branch of linguistics that deals with the study of meaning, (2), the study of the relationships between signs and symbols and what they represent" (Collins Dictionary, 1981., p. 1179). As such, there must exist semantic and linguistic commonalities across all conceptions and examples of security. Again, deferring to the words of Socrates, "we are searching for that thing which is the same in all these".

Accordingly, the proposition of this study is that there does exist thematic facets that can be extracted from this broad discourse to denote the term security and seat the

study. Consequently, it is argued that a thematic analysis of the examined literature leads to the assertion that both philosophically and functionally the axiomatic meaning of security can be understood in relation to conditions of well-being for values in the face of threat. Hence, the study denotes security as:

[Security is] philosophically, a communal theory of survival and conditions of human and entity existence; where functionally it is the pursuit of this philosophy underscored by conceptions of risk. The cover term Security denotes the pursuit to protect defined values against real and perceived threats to them…where the functional word security relates to the degree of control or influence over an environment to achieve protection.

Security in terms of control or influence is achieved through adaption, accordant with its biological definition. This in the words of Freidson (1973), refers to the evolutionary means of survival through changes in physical characteristics and ways of behaving that have proven viable in an environment in the face of conditions and constraints in which they happen to exist.

Thus, security denotes protection from the adverse effects of threat, and functionally it's the pursuit of such protection. Congruous with the writings of Wolfers (1952) and Maslow (1970), security as a referent to values elucidated in survival and conditions of human existence, including the retention of belongings is a very crucial societal concept. Mill's (1910) work on society recognised this view, stating that security of the person and property, along with equal justice between individuals are the first needs of society, and the primary end of government (p. 355); from the beginning of human kind to the advanced society of today that security has always been a concept essential for survival (Mill, 1936, p. 50). Security is about survival at a global, National/State, organisation or group and individual levels.

Security as a subject is concerned with very important matters, be it physical survival, economic survival or a state of enhanced being. The function of security is about providing wellbeing consistently, resulting in a stable-predictable environment to pursue higher order objectives. When threats are not managed, accordant with Maslow's work, a reversion or refocus in pursuits occurs until security is again achieved to a degree where higher pursuits can be a priority pursuit again. Security exists in a context

but its denotation is the same. Its pursuit also exists in a context where various means are utilized to obtain a desired state. Such means exist across all contexts or many of them and they can be grouped and organised accordingly. The context of the study lies in the pursuit of wellbeing in terms of survival and the retention or integrity of assets through the means of physical security practices as a more focused area of foci within the broad societal domain of security.

Nonetheless, it must also be acknowledged that security, regardless of context, is a more relative rather than absolute term (United Nations, 1986, p. 2), epitomised as entwined in layers of values (Baldwin, 1997). For instance, Corkill and Coole (2013, p. 144) stated that security is achieved utilizing a control thesis, which holds that without control, or at least influence there can be no security. Consequently writers such as Wolfers (1952, p. 494) and Stone (2009, p. 8) make the point that absolute security is never going to be attained, as absolute power (Baldwin, 1997) and therefore total control is not achievable. Ullman's (1983, p. 1) writings acknowledged this very view reminding us that a state or level of security towards protecting values must be balanced against other values, as often measures implemented to achieve security (control) can be experienced as a burden (Wolfers, 1952, p. 488). As such, efforts are made to keep such control at the lowest level required, which will provide what is considered proportional protection within a context (Wolfers, 1952, p. 488). In 1952 Wolfers (p. 494) expressed that a security balance is required accordant with the economic law of diminishing returns, where the gain in security no longer compensates for the added cost of attaining it; this point still holds today. Thus, while security philosophically is a communal pursuit, at a functional level it is about establishing the right level of cultural influence or control within a context commensurate with costs benefits accordance to conceptions of risk.

Security, especially physical security, inhibits or facilitates actions, and as a construct has a long crucial history with mankind (Maslow, 1970, pp. 35-46; Underwood, 1984, p. 3; Manunta, 1997, p. 11), with its universal need unquestionable (O'Shea & Awwad-Rafferty, 2009, p. xv-xviii). In pursuing security, humans' survival as a species and as entities within the global community is determined by their ability to organise and adapt as a group to develop a degree of influence or control over an environment. Such control is towards protecting values as referents to people, possessions or beliefs from

harms in the face of real and perceived threats. Such threats stem from malevolent human actions and conditions that may result in such actions. Security is a concept essential for survival and also provides a better quality of life.

Further framing the study is the acknowledgement that security across contemporary society is more recognised and defined by its euphemistic category contexts rather than in terms of broader conceptualizations of values and control, regardless of the point that security concerns values and is achieved through control. Furthermore, vocationally security is considered as an array of various fields in which it is applied (Table 1.2) and within these contexts are various applications to achieve security functionally. Thus security is conceptualized as an umbrella term (cover term) in relation to its contextual pursuit, rooted within its euphemistic or adjective categories. Accordingly the pursuit of a state of security as an occupational domain is acknowledged within the study as taxonomy of professional or occupational subdivisions, where security is philosophically understood implicitly and functionally pursued contextually.

Security as a domain discipline explained in taxonomic terms means that regardless of its crucial and historical basis, its diversity along with academic youth, especially in the non-traditional paradigm, means that its holistic knowledge domain is yet to achieve the formal status of traditional professions and their supporting academic disciplines. For instance, to date, no study has ever demonstrated an all-encompassing knowledge base that captures the depth and breadth of the security domain. As highlighted by Smith and Brooks (2013, pp. 1-2), when compared to disciplines such as medicine and law, security lacks validity in significant characteristics, including a well-defined formal knowledge structure and agreed skill sets, largely due to its infancy and diversity (p. 16).

Yet irrespective of security's diversity and its limited explicit knowledge structure, corresponding with security's cruciality and its functional embeddedness within contemporary society, an emerging occupational group is the modern day security professional (Section 1.4). Thus, this emerging professional must theoretically be educated or trained and experienced in protecting modern society from the multifaceted security centred threats that pose a risk to survival, property or threaten conditions of existence for nations, states, organisations and groups, and individual people. Though

pragmatic questions remain, given the breadth and depth of the domain. What constitutes a security professional? What is their occupational boundary and commensurate knowledge basis along with competencies and supporting formal educational requirements?

2.3 Conceptualising a modern day professional

The study is also seated within the concept of the modern day professional. Therefore, informing the notion and embodiment of the modern day security professional is the literature of professionalism. According to Abbott (1988, p. 3), historically the professions and its supporting embodiment professionalism as a concept is derived from medieval times, from the guilds. However, clearly defining a profession is somewhat controversial (Cogan, 1955, p. 105). As early as 1915, Flexner's work sought to define the concept of professionalism, asserting that a profession is characterised by six criteria: (1) intellectual operations coupled with large individual responsibilities (2) raw materials drawn from science and learning (3) practical application, (4) an educationally communicable technique, (5) tendency towards self-organization, and (6) increasing altruistic motivation (Flexner, 1915). However, in 1955 (p. 105) following on from Flexner's work, Cogan's work avowed that "there is still no universal definition of a profession", an assessment which arguably still remains today.

The work of Jaques (1989) echoed that professionalism as a concept relates to the stratification of work in society. Jaques (1989, p. 15) articulated professional work as the use of discretion and judgement in making decisions, in carrying out a task, backed by knowledge, skills, temperament, and wisdom, and driven by values. According to Jaques (1989, p. 23) work, professionalism relates to problem complexity where complexity is defined in terms of the number of variables operating in a situation, the clarity and precision with which they can be identified and their rate of change. Professional work has to do with higher strata problem solving; problems start with something you value, need or want (goal) that is not immediately available and the development of the processes to achieve the desired goal. Only as problem complexity is reduced can tasks be delegated to lower work strata (Jaques, 1989, p. 34).

Such views were summarised in the earlier and influential work of Wilensky (1964, p. 138) who expressed that, "there are two criteria for professional groups, (1) the job of

professional groups is technical-based on systematic knowledge or doctrine acquired through long prescribed training (cognitive), (2) and that the professional adheres to a set of professional norms" (normative). Nonetheless, the more recent work of Eraut (1994, p. 1) contends that regardless of individualistic account, the profession's explicit conceptual boundary is still poorly defined. Eraut's (1994, p. 1) work contends that as opposed to a true entity the contemporary concept of professionalism is somewhat more of an ideology that in the words of Larson (1977, p. x) embodies varying attributes amongst authors, but generally include cognitive, normative and evaluative dimensions.

According to Larson (1977, p. x) a profession's cognitive dimension is centred upon the knowledge and techniques in which this knowledge is applied. The normative dimension covers the service orientation of the profession, underscored in appealing values including ethics or trustworthiness, integrity, autonomy and reliable standards. Evaluative refers to the profession's comparison to other occupations in terms of its prestige (Larson, 1977, p. x). Jaques bridged these views together; defining cognitive processes as "the mental processes by which you take information, pick it over, play with it, analyse it, put it together, reorganise it, judge and reason with it, make conclusions, plans and decisions and take action". In professional work you exercise discretion, judgement and decision making, within limits, in carrying out tasks: driven by your values, and bringing your knowledge, skills, wisdom and temperament into play (Jaques, 1989, p. 33).

Cogan's, Wilensky's and Jaques' works are still influential today; it is within these embodiments that the most prominent professions of medicine and law are held up as the ideological symbol of professionalism (evaluative) (Eraut, 1994, p. 1; Axt, 2002, p. 142). As Gillespie (1981, p. 371) notes, although there is considerable debate over 'what is a profession', there is no debate that both medicine and law are professions (high prestige). Acknowledging the cognitive dimension of professionalism, Cogan's (1955, p. 107) work further articulated that a profession is "a vocation whose practice is founded upon an understanding of the theoretical structure of some department of learning or science, and upon the abilities accompanying such command". A viewpoint later supported by Freidson (1973, p. 40) who further exclaimed that in terms of professional work, scientific knowledge is the most respected in contemporary society.

The work of Freidson contended that many professions assert as evidence of their professional status their possession of expert knowledge stemming from scientific basis. For example, according to Freidson (1973, pp. 40-41) medicine and occupations such as medical technology and nursing lay claims to portions of biology and the physical sciences in their assertion of professional status. Engineering rests its professional status on its foundations in the physical sciences and mathematics. Nevertheless, it is also acknowledged that professional status can rest on claims upon knowledge of some arbitrarily constructed model of social organisation, such as the law profession, where the knowledge is not scientific per se, but is complex and critical for overcoming problems that arise in modern society, presenting the notion of esoteric or abstract knowledge as a further basis for professionalism.

Knowledge-based views underpinning professionalism resonate within the literature. As the writings of Freidson (1973b, p. 173) express, professionals possess processed knowledge based on measurement, systematic observation, and scientific theories. The work of Olufs (1985, p. 29) supports this view; asserting that instrumental in the existence of a profession is a formally established body of knowledge as a cognitive underpinning of its practice. A view unremitting by Eraut (1994, p. 102) who explains that within the professionalism criteria sit two primary bases for establishing professional specialisation. These include a profession's substantive field of knowledge that is professed to be of their command, and its technique of production or application of that which the professional claims mastery.

Congruent with the cognitive constructivist view (Section 1.6), all reviewed authors present a knowledge-based view characterising professionalism in relation to professional work. Knowledge was defined in Section 1.2.1 as the: (1) the facts or experiences known by a person or group of people, (2) the state of knowing, (3) consciousness of familiarity gained by experience or learning, (4) erudiation of informed learning, (5) specific information about a subject, and (6) understanding. The work of Eraut (1994, p. 103) highlights that such professional knowledge is divided into three salient categories including (1) discipline based concepts and theories derived from bodies of coherent, systematic knowledge, (2) generalizations and practical principles in the applied field of professional action, and (3) specific propositions about particular cases, decisions and actions, referred to as reflective practice.

Concepts in an occupational sense can be understood as something which can be conceived, a notion, an idea, thought or device (The Oxford English Dictionary, n.d.) a mental representation of a thing or class of things so that an individual can decide whether a specific stimulus is an instance of that object or class of objectives and act on the basis of that judgment (The Cambridge Dictionary of Psychology, 2009, p. 123). Whereas, an occupational theory can be understood as (1) a conception or mental scheme of something to be done, (2) or of method for doing it; a systematic statement of rules or principles to be followed (The Oxford English Dictionary, n.d.). However, a theory is also defined as a conjecture or opinion on a topic (The Cambridge Dictionary of Psychology, 2009, p. 542). Then a principle is the chief or main part, point or element of something…a primary or fundamental point of a subject, upon which the rest depends…a common (The Oxford English Dictionary, n.d.).

Bringing such literature together as organised professional knowledge, Jaques (1989, p. 34) expressed the view that "all knowledge is verbally articulated, and is held in memory". You may sense something, but "if you cannot state it, you do not know it". Therefore this definition of knowledge is applied in the professions' literature within an individualistic-professional sense, relating to masters of a field; knowledgeable about technical concerns and schooled in the judgements required in their application.

2.4 Cognitive dimensions of professional knowledge

The reviewed literature has expressed the importance of cognitive attributes, specifically specialized knowledge as the currency for producing professional work and ultimately designation as professionals. Yet few authors have explored where this knowledge comes from and how it gets established as recognised knowledge; and how its development and utilization become organized, evaluated and controlled (Freidson, 1973, p. 28). Within the literature is the view that a profession's cognitive dimension is centred on the formal body of knowledge and techniques which the professionals apply to their work (Larson, 1977, p. x).

The work of Epstein and Hundert (2002, p. 227) explained that the cognitive dimensions of professional competence include a component of acquiring and using knowledge to solve problems. Such competence is underpinned by fundamental facets including core knowledge, using resources (e.g. published evidence, colleagues) along

with using tacit knowledge learned from experience coupled with abstract problem solving skills. Fittingly, the earlier work of Abbott (1988, p. 323) highlighted that professionalism has been the main way of institutionalising individual's expertise, where the technical knowledge within expertise can be formally codified (Oakeshott cited in Eraut, 1994, p. 65). Acknowledging such a process, Brooks presented the argument that "security experts individually hold a rich knowledge structure" which can be captured (2007, p. 1).

Thus, the emergence of a profession is predicated on the concept of individual expertise, which moves from an individualistic position, to a group phenomenon. Individual expertise is considered within the work of Ericsson and Charness (1997, p. 6), who claim that expert performance within a domain is defined as consistently superior performance on a specified set of representative tasks for the domain that can be administered to any subject. Expertise is viewed in terms of reasoning ability and knowledge (heuristic and compiled) (Patel & Ramoni, 1997, p. 76). In addition, Ericsson and Charness (1994, p. 731) define experts as individuals who are performing at least two standard deviations above the mean level of performance in their domain population. The mechanisms of expertise and expert performance reflects the complex, domain specific cognitive structures and skills that performers have acquired through their incremental accumulation of knowledge and skills over a decade of intense experience (Ericsson & Charness, 1997, pp. 4-5). That is, accordant with Section 1.6, professional knowledge is built on the foundations of existing knowledge.

Congruent with the constructivist approach (Section 1.6), studies have shown that a large organized body of domain knowledge (technical knowledge) is a prerequisite to expertise (Bedard & Chi, 1992, p. 135). That is, experts have a greater quantity of domain-relevant knowledge than do novices and it is better organised than novice's structures. In addition, experts perceive more meaningful structural patterns in their respective domains than non-experts, whereas novices perceive random or disconnected structures or patterns within and between cases (Johnson, 2003, p. 58). Furthermore, while expert knowledge is argued to be more organized, accessible, functional and efficient than that of novices, Bedard and Chi (1992, pp. 135-136) emphasize that an expert's knowledge is also cross referenced with a rich network of connections amongst concepts. According to Bedard and Chi (1992, p. 135) within the context of professional

knowledge what is crucial is the manner in which it is organized that makes it more accessible, functional and efficient.

2.5 Individual professional expertise

Expertise underpins the concept of professionalism, which as a subject of research resulted from developments in artificial intelligence (AI) and cognitive psychology (Chi, Glaser and Farr, 1988, p. xv). The study of expert performance is considered across two broad discourses including a physiological (unmodifiable-innate) or talent-based view and cognitive factors (modifiable-mental factors), which influence the achievement of expert performance (Ericsson & Charness, 1994; Chi, Glaser & Farr, 1988; Tynjala, 1999). The focus for this study is on cognitive factors as expertise drivers based on the argument that professional competence includes a cognitive dimension including core knowledge, using tacit knowledge and personal experience, self-directed acquisition of new knowledge, using resources and learning from experience (Epstein & Hundert, 2002, p. 227) that is modifiable over time.

Ericsson and Kintsch (1995, p. 221) describe cognitive processes as a sequence of states or thoughts. For example, the works of Degroot (1966) and Simon and Chase (1973) showed that specialised structures of knowledge were strongly implicated in expertise (Chi, Glaser & Farr, 1988, p. xv). Within the context of professional knowledge, Sternberg's (1997, p. 159) views are that expertise can be considered as a domain-specific multidimensional prototype underpinned in varying degrees by seven attributes:

1. Advanced problem solving processes;
2. A great amount of knowledge;
3. Advanced knowledge organisation;
4. An ability to use knowledge effectively;
5. Creative ability; involving creating new knowledge on the basis of knowledge that one already knows;
6. Automated actions; and
7. Practical ability (p. 150).

The reviewed literature highlights that salient within the cognitive literature of expertise is the concept of expert knowledge within a particular domain and its organisation

(Bedard & Chi, 1992; Ericsson & Charness, 1997; Sternberg, 1997; Zeitz, 1997; Tynjala, 1999). Research on the development of expert knowledge is of fundamental importance towards understanding the acquisition of expertise (Tynjala, 1999, p. 359) and specifically as it relates to this study. Professional knowledge is often broken down into three salient components namely formal knowledge, practical knowledge and self-regulative knowledge. Formal knowledge refers to declarative knowledge often known as explicit, factual or propositional knowledge. Such knowledge is considered to play a major role in education and constitutes the core of professional knowledge competence (Tynjala, 1999, p. 359). This knowledge is the province of the cognitive domain (Carter, 1985, p. 139). Practical knowledge, often referred to as procedural knowledge, is that knowledge structure which manifests itself as skills or 'knowing-how' and is considered more personal or tacit in nature. Self-regulative knowledge consists of meta-cognitive and reflective skills that individuals use to monitor and evaluate personal actions (Tynjala, 1999, p. 359).

2.6 Knowledge-based views of domain expertise acquisition

A recurring theme within the literature is that professionalism is predicated on the authority of expertise (Freidson, 1973, p. 25). As such, central to the proposed outcomes of the study is the knowledge–based views of expertise acquisition that incorporates a human information processing or skills approach (cognitive). This explains exceptional performance in terms of knowledge and skills and posits that outstanding performance results from incremental increases in knowledge and skill (constructed) due to the extended effects of learning and experience (Ericsson & Charness, 1997), which builds over time. Within this school of thought it is argued that experts acquire memory skills to meet specific information processing and accessibility demands in specific activities (Ericsson & Charness, 1994, p. 736). According to Ericsson and Charness (1994, p. 736) acquired memory skill (Skilled Memory Theory and Long Term Memory) accounts for the superior memory of domain specific knowledge of experts. Experts develop domain specific memory skills that enable them to store domain relevant information in their Long Term Memory (LTM), circumventing general Short Term Memory (STM) capacity constraints.

Ericsson and Charness (1997, pp. 13-16) contend that a critical aspect of expert's working memory is not the amount of information individuals have stored per se, but rather how they have stored and indexed their information for retrieval from their LTM. Contemporary views of human memory emphasise two distinct forms of storage systems, referred to as Short Term memory (STM) and Long Term Memory (LTM). Short Term Memory is characterised by a limited storage capacity with a memory span limited to around 7 different digits or consonants and slightly fewer (5-6) colours, visually presented geometric designs, and words. This is summarised as...STM has the capacity to retain 7 plus or minus 2 symbols or chunks of information. As such, for information to be stored permanently it must be placed in LTM an unlimited and permanent storage system (Ericsson and Chase, 1982, p. 607).

Nevertheless, information in LTM can only be retrieved through precise retrieval cues, where storage and retrieval of information in LTM for normal people requires considerable effort and time. Storage in LTM is assumed to be primarily associative, relating different items to one another and relating items to attributes of the current situation (current context). According to Ericsson and Kintsch (1995, p. 212) the primary bottleneck for retrieval from LTM is the scarcity of retrieval cues that are related by association to the desired item stored in LTM. However, to perform complex cognitive tasks people must maintain access to large amounts of information. In working or professional contexts individuals require accessible information that changes as the individual continues with their task (constructive), and are often referred to as working memory, or as Ericsson and Kintsch (1995, p. 211) express, Long-Term Working Memory (LT-WM).

It is premised that individuals can acquire domain-specific memory skills, which allow them to acquire LT-WM extending their working memory for a particular activity. LT-WM is found for many types of expert performance and is the normal mode of expert processing (Ericsson & Kintsch, 1995, p. 211). LT-WM is acquired in specific domains to meet specific demands imposed by a given activity on storage and retrieval and must therefore be considered in the context of specific skilled activities (p. 221). Again, it is emphasised that a critical aspect of experts' working memory is not the amount of information stored, but rather how the information is stored and indexed in LTM. Bruner (1977, p. 24) highlighted, that human memory research supports that unless

detail is placed into a structured pattern, it is rapidly forgotten…detailed material is conserved in memory by the use of simplified ways of representing it, and such simplified representations have what is called a regenerative character.

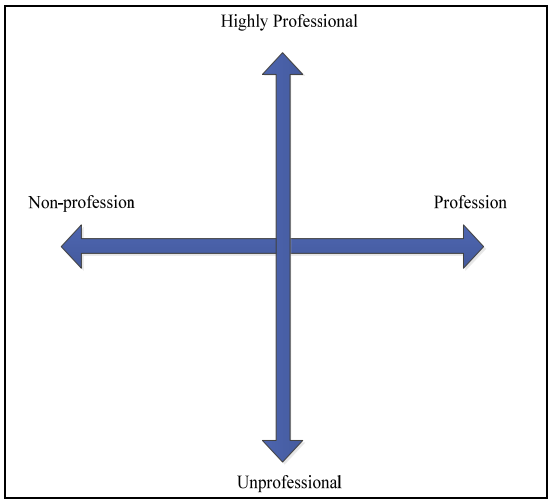
Emphasizing the importance of this theoretical foundation to expertise and domain professionalism, Smith (2002, p. 21) explains that the network of relations among concepts in LTM constitutes the substantive or subject matter structure of a particular domain. A view supported in the underlying premises within Bloom's Taxonomy of Educational Objectives which acknowledged that experts and novices differ not only in the amount of knowledge they possess, but also in the organisation and accessibility of that knowledge. Such differences in knowledge structures are premised to be based around four principles:

1. The knowledge of novices is structured around the main phenomenon in a domain, while that of experts represents phenomena in relation to higher order principles;
2. For the expert, these principles are represented in the form of problem-solving procedures as well as in the form of declarative knowledge;
3. Moreover, such procedural representations include specifications of the conditions under which principles are applicable. Thus, the principles are connected with the phenomena to which they can be applied and even the concrete components of the phenomena; and
4. Experts' knowledge structure, in contrast to those of novices, also includes understandings of the goals and structures of the domain (Anderson & Sosniak, 1994, p. 61).

Thus, accordant with the writings of Smith (2002, p. 21) and Brooks (2007, p. 1) security experts as individuals personally hold a rich knowledge structure in their LT-WM. Congruent with such a view, the earlier work of Cogan (1955, p. 110) highlighted that professionalism can exist in a group phenomenon or it may be achieved individually. Then the writings of Ritzer 1973 (cited in Freidson, 1973, p. 60) further express that the "culture and technique, the etiquette and skill of a profession, appear in the individual as personal traits, where all occupations may be placed on a continuum ranging from non-professions at one end to the established professions at the other end"

(Figure 2.4). Once you pinpoint the position of an occupation on this continuum, the question that remains is the degree of professionalism of the individuals within. For example, medicine falls on the professional end of the continuum, but individually doctors can vary in their degree of professionalism.

Figure 2.4 Dimensions of professionalism



Such a notion applies at the nonprofessional end of this continuum, whereby the occupational category of taxi driver is not regarded as a profession. However, some individual taxi drivers may be regarded as professional because of their knowledge of cars and the city (cognitive attributes), or their commitment to helping people (normative attributes). Thus, the individual in a professional occupation may be considered non-professional at the individual level if they do not have the intelligence to understand the theory that underlies their occupation. There is a relationship between occupational and individual professionalism (Figure 2.4), but the relationship is not perfect (Freidson (1973, pp. 60-61). Applying such literature to the security domain, it can be claimed that individually security experts can be professional. However, as a group they lack public acknowledgement as professionals. It is within this contention that Brooks postulates that such individual's professional knowledge can be captured (2007, p. 1); where professionalisation has been the main way of institutionalising such expertise and attitudes towards establishing a profession (Abbott, 1988, p. 323), achieving formal codification.

2.7 Professionalisation

Eraut (1994, p. 1) argued that the concept of professionalism lies in the social control of expertise, where according to Abbott (1988, p. 323) the concept of professionalism has been the salient means of institutionalising individual expertise in industrial countries. Thus, many proponents of professionalism view knowledge-based expertise as a prime source of professional power and influence (Eraut, 1994, p. 2), and therefore prestige (evaluative). From this ideological standpoint, professionalisation is the process or path to professionalism (Larson, 1977, p. xvi) that produces an occupational group of focused abstract skill sets, stemming from systematic knowledge where its capture requires extensive training (Abbott, 1988, p. 7).

The writings of Bruner (1977, p. 17) recognised and separated two prominent means in which learning serves its future employment to produce work outcomes. First is the specific applicability to tasks that are highly similar to those in which original learning was geared to perform, referred to as specific transfer or training. The second way in which earlier learning renders later efficient occupational performance is through nonspecific transfer (learning abstractions), or more accurately, the transfer of principles and attitudes. In essence such learning consists of initially learning a general idea, which can then be used as a basis for recognising subsequent problems as special cases of the idea originally mastered. This type of transfer is at the heart of the higher educational process, as opposed to training. That is the continual broadening and deepening of knowledge in terms of basic ideas, this type of learning is what underpins the professional (Abbott, 1988, p. 7).

In 1964 Wilensky's persuasive work (1964, p. 137) recognised that many occupations pursue professional status. It is within this societal context where the current discourse towards defining the concept of the security professional and identifying their core professional competencies lies in the view that professions dominate contemporary society. Professions heal our bodies, measure our profits and save our souls (Abbott, 1988, p. 1), and now they manage our security risks (Australian Interim Security Professionals Task Force, 2008). Together they make up an interdependent system where each profession has its activities under various forms of jurisdictional work boundaries (Abbott, 1988, p. 2).

Accordant with cognitive dimensions of professional competence, early works established and accepted that professions were organised bodies of occupational workers. These workers applied esoteric knowledge in the form of expertise to particular activities to produce professional work. They had elaborate systems of instruction and training, together with entry by examination and other formal requirements (Abbott, 1988, p. 4). Emerging from this basis, now a profession is seen as an occupational group or the body of people in such an occupation (Abbott, 1988, p. 7; Collins Dictionary, 1981, p. 1029), with some special skill, one of abstract nature (non-specific transfer) requiring extensive training that is refined through practice (Abbott, 1988, p. 7).

Wilensky (1964, p. 142) noted that while many occupations assert a claim for professional status, they find their claims not honoured by the greater community. Freidson (1970, pp. 3-4) acknowledged this phenomena highlighting that virtually all self-conscious occupational groups apply it (profession) to themselves at some time or another, either to flatter themselves or to try to persuade others of their importance; but they are not recognised professions. Abbott's writings (1988, p. 70) considered this responsive to the theme that self-labelling occupational groups do not define professions; the public and legal arenas, through supported explicit jurisdictional claim, define them. Therefore, professions are a social designation and have no real standing as long as they are implicit or self-professed. This very viewpoint was acknowledged for the security domain in the writings of Axt (2002). Congruent with this line of thinking Wilensky's (1964, p. 145) work voiced that the lay public cannot accept the need for special competence in an area where everyone is an expert. In this sense, Abbott (1988, p. 7) insists that professional knowledge is not occupational knowledge applied in a purely routine fashion (specific transfer), but rather knowledge that requires revised application, case-by-case (non-specific transfer) over time. Furthermore, of significant importance in the professions is the concept of jurisdictional control to maintain professional standing.

The literature on professionalism highlights that a profession must control its technique or its abstract knowledge system, where here practical skills grow out of this cognitive abstraction (transference of principles), to maintain its jurisdictional authority. Barnett (1994, pp. 34-35) embraces Abbott's (1988, p. 7) views, declaring, "professionals are

academically qualified people in control of a body of knowledge that is denied to their client and secure remuneration for services rendered to said clients" (Barnett, 1994, p. 34). Furthermore, it is emphasised within the Collins Dictionary (1981, p. 1029) with great skill or competence, and the furtherance of the profession. According to Larson (1977), Tawney stated:

> [Professionals] may, as in the case of the successful doctor, grow rich; but the meaning of their profession, both for themselves and for the public, is not that they make money, but they make health, or safety, or knowledge, or good government, or good law…[Professionals uphold] as the criterion of success the end for which the profession, whatever it may be, is carried on, and [subordinate] the inclination, appetites, and ambition of individuals to the rules of an organization which has its object to promote the performance of function. (Tawney cited in Larson, 1977, p. 58)

The work of Marutello (1981, pp. 248-249) also reflected such a view, stating "the primary intrinsic or compelling aspects of an enterprise that make it eventually and ultimately evolve into a profession include the three elements of Cruciality, Mystique, and Denouement". Here cruciality means that the occupation in question has an almost life-or-death fateful relationship to its clientele, the public or employers. Crucial matters are those that are defined by an individual as deadly serious. Mystique arises out of cruciality, where the person with the crucial problem seeks help from somebody believed to have a great deal more knowledge than the lay person to solve it. This someone is seen to be in possession of technical skills, expertise or having specialized advanced training, underpinned by a body of knowledge not available to the person seeking resolution. Denouement is the resolution of the critical matter and involves the application of the implicit concepts of the previous two elements and becomes the basis for the complete sematic definition of a profession. For instance, Marutello (1981) states:

> An individual engages in a profession when there is the application of a body of knowledge or principles seemingly available only to the select (Mystique). Which has been 'scientifically' or practically proven to be applicable to special contexts to bring about certain defined and largely

> predictable or hoped for outcomes over a relatively short period of time (Denouement) about very vital matters for particular individuals (Cruciality). (Marutello, 1981, p. 249).

Fitting with such analyses, security as a concept has been well established as a vital human need (Section 2.1) (Cruciality), where security's means of reducing threat related risks is broad and complex (mystique) and so its embodiment professionally can arguably be allied with Marutello's (1981, pp. 248-249) discourse. For instance, through Table 2.1, Marutello's defining elements of professions are aligned with the traditional professions of medicine and law adding the emerging profession of security in the non-traditional sense.

Table 2.1 Elements defining three professions (adapted from Marutello, 1981, p. 250)

Profession	**Mystique**	**Cruciality**	**Denouement**
Medicine	Body of medical knowledge accessible only to the select	People are sick and want to be cured	Application of mysterious principles to very concerned sick individuals with the high predictability of bringing about a resolution over the short term
Law	Body of legal knowledge accessible only to the select	People are in big trouble and want to get out of it	Application of mysterious principles to very troubled individuals and (largely) predictably bringing about a resolution over the short term
Security	Body of security knowledge accessible only to the select	People or assets of value are in danger and protection from threat is sought	Application of mysterious principles to very concerned individuals, groups or organisation to ensure their survival or quality of life

In this sense, congruent with the writings of Wilensky (1964, p. 138), Barnett (1994, p. 35) expressed the existence of a professional client relationship embedded in trust where their client expects the solicited professional to exploit his or her specialised knowledge in somewhat predictable fulfilment of their interests (Table 2.1). For this reason, professionalism places central emphasis towards a distinct, formal body of knowledge that aims to achieve predictable outcomes. As such, according to Eraut (1994, pp. 1-3)

some occupations, including teachers and social workers, which have had a long history of professionalisation, have been constrained in their professional progress, status and salaries, partly because they have not been able to explicitly articulate their distinct knowledge base, or control entry.

These writings highlight that professionals' concerns are towards the pragmatic usefulness of their jurisdictional knowledge (Table 2.1) (Eraut, 1994, p. 3) to produce professional work. Such usefulness includes both academic and practical aspects (Griffiths, Brooks & Corkill, 2011, p. 35). A profession's academic basis therefore defines its jurisdictional practice (Martin & Guerin, 2005, p. 16; Morris, et al, 2006, p. 710; Smith & Brooks, 2013, p. 16), reiterating an academic versus practical dichotomy to professionalism. This dichotomy of professionalism further informs the concept of the security professional, as this very dichotomy led Fox (1994) to emphasize the requirement to separate the science or learning of a discipline with the profession of a discipline.

In his review of the psychology profession, Fox (1994, p. 202) viewed the profession of psychology as being concerned with human problems arising from or associated with purposive behaviour that is understandable or potentially understandable through scientific knowledge in psychology. Yet, the science of psychology is concerned with understanding the behaviour of human beings…"where, professional psychologists are considered to be persons who have extensive expertise in the development and application of service to the public based upon domain relevant scientific knowledge of human beings" (p. 202).

Fox's (1994) analysis is more recently emphasized in the legal expert literature of Freckelton and Selby (2013). Congruent with the educational insights of Barnett (1994, pp. 34-35) and Abbott (1988, p. 7) for professionals, Freckelton and Selby (2013, p. 1051) consider that science-based domain experts must have the qualifications, experience, and training that form the basis of their claimed expertise. For example, in contemporary times Freckelton and Selby (2013, p. 1051) state that within the expert domain of fire investigations, an area previously dominated by those who learned 'on the job', is now in a position where "unqualified experts are becoming less acceptable and less common". From their legal standpoint Freckelton and Selby (2013, p. 1052)

assert that in the interest of scientific accuracy, credibility and justice it is reasonable to expect an expert to have completed the relevant academic study accordant with the science that underpins their domain.

Furthermore, accentuating Abbott's (1988, p. 7) and Barnett's' (1994, p. 34) analyses that professionals are academically qualified people, Freckelton and Selby (2013, p. 1052) deem it a necessity to achieve the relevant undergraduate qualifications as now many post graduate programs afford for prior learning to fast-track students into tertiary courses. This means it is possible to obtain a post-graduate qualification without being a graduate, or a higher degree without first obtaining a lower degree. This can cause problems as the underpinning sciences are not acquired through practical experience. Although the dichotomy emphasises experience conversely cannot be acquired through academic knowledge (Freckelton & Selby, 2013, p. 1052). In bridging the literature together, Fox (1994, p. 202), states that "as a minimum professionals apply validated techniques where a profession is defined according to its verified knowledge base of the science or learning on which it is founded.".

The reviewed literature of Bowen, 1955; Cogan, 1955; Wilensky, 1964; Mosher, 1968; Gillespie, 1981; Kline, 1981; Marutello, 1981; Olufs, 1985; Barnett, 1994; Eraut, 1994; Abbott, 1988; Wilson & Oyola-Yemaiel, 2001; Borodzicz & Gibson, 2006, and the Australian Interim Security Professionals Task Force, 2008) highlighted that to date definitional and jurisdictional ambiguity shrouds the concept of the contemporary security professional. Nevertheless, there are specifically accepted core criteria that define a professional including:

1. A body of knowledge or techniques;
2. Formal; standardized education; training and experience;
3. A representative organisation with the purpose of professionalisation;
4. Fees based on service to clients or customers with priority given to service rather than financial returns; and
5. An ethical code of conduct and broad-based responsibility.

Reflecting on the reviewed discourse objectively, security does not stand up as a profession in the traditional sense as few outside the domain recognise its professional

stream. As Criscuoli (1988, p. 102) notes, the general public does not perceive security as a profession. Petersen (2014, p. 80) clarifies this position well, stating traditionally common education is the seed to a profession whereas security in contrast draws its coherence not through such codified body of knowledge but through an informal community of practice. However, its professionalisation process is directly allied to common educational backgrounds and certification programs. Nonetheless, The Australian Interim Security Professionals Task Force (2008) designated security professionals as those groups of people working at the senior end of the operational sector and in the strategic sector of the Security Industry. However, this is a broad statement, lacking deeper qualification and arguably broader public acceptance. Especially in light of the view that security education is often too broad and too shallow, perhaps due to a lack of clear jurisdictional boundary and supporting structure.

Therefore, accordant with the reviewed literature the study must reflect that a professional, as a minimum, is somebody who is academically qualified and specially trained, in a formal manner, in the liberal arts or sciences of which their jurisdictional domain is fashioned. This learning forms a substantive field of knowledge in which they are in command of, and apply validated techniques to solve society's security related problems (Wilensky, 1964; Abbott, 1988; Barnett, 1994; Eraut, 1994; Fox, 1994; Freckelton & Selby, 2013). Professionalisation is the process an occupational group goes through to establish their group status as professionals accordant with the verified bases of their learning.

2.8 Conclusion

This chapter presented the foundational literature supporting the study. The chapter commenced with a philosophical yet functional discussion of the term security (2.2), which underpins security professionalism. Then, Section 2.3 conceptualized what a professional is, supported by cognitive dimensions of professional knowledge (2.4) and individual professional expertise (2.5), which was supported by knowledge-based views of domain expertise acquisition in Section 2.6. This literature was clarified through a discussion of the professionalisation process in Section 2.7. These discussions supported the view that security is a vital and legitimate construct (cruciality) for a free and civil society.

The chapter highlighted that professions and professionals apply validated techniques according to its verified knowledge base of the science or some complex department of learning on which it is founded (see Sections 2.4, 2.5 and 2.6). Such experts in a field are argued have an implicit knowledge base that can be captured, codified and integrated to achieve a body of knowledge as a formal knowledge system.

Chapter 3: Jurisdictional boundary and education literature informing the study

3.1 Introduction

This chapter presents the occupation-jurisdictional and educational literature informing the development of a cultural body of knowledge for physical security professionals. Section 3.2 positions the physical security professional within the profession's literature, where Section 3.3 establishes a clear jurisdictional boundary for the study. Section 3.3 discusses defining a professional person accordant with his or her body of knowledge, where section 3.5 presents professional status within the security domain. Section 3.6 discusses the ambiguity of security education in relation to this literature. Section 3.7 discusses the concept of a higher education curriculum for security professionals, whereas Section 3.8 presents the curriculum and the typologies as a vehicle for the broader recognition of security science.

The chapter also explains the current debate of higher education's roles for security professionals in Section 3.9, posing the question: does security possess a formal body of knowledge? Section 3.10 of the chapter presents the literature supporting focused research undertakings as a means of formally codifying occupational bodies of knowledge. This literature is fused together in Section 3.11 through a reflection, articulating how the reviewed literature influences the study's enquiry boundary, research objectives and questions, and its methodological approach. The chapter concludes with Section 3.12.

3.2 Conceptualising the physical security professional

The concept of security is asserted to be a theory of both survival and conditions of human and entity existence (Section 2.1) that is multidimensional and ubiquitous in nature. Because security is so multidimensional there is no single methodology to be applied in its pursuit. The writings of Gillespie (1981, p. 19) highlight that for such umbrella or taxonomic domains it is a technical misnomer to call them professions, as they are actually a set of professions. Within such umbrella-like domains (sets), there are usually smaller sections designed to relate more specifically to the differentiated needs of the broader membership (Gillespie, 1981, p. 19). Thus, based on the reviewed literature the study contends that the methods for achieving security must stem from the

knowledge that underpins professional sets (practice areas) within, and across the broader domain (euphemistic categories) of security. Where congruent with Manunta's (1997, p. 19) views in its operational sense, security includes the functions and activities aimed at preventing unacceptable losses and damages to those tangible and intangible assets considered worthy of protection.

In this sense, Manunta (1997, p. 1) expressed a long held acceptance that, congruous with other professional domains (Section 2.2.2), security is an organised complex of specialised functions, which embodies well-identified principles, means and methods whose validity and consistency derive from millennia of experience and sound methodology. While such literature identifies a historical yet somewhat implicit or fractured explicit nature to security, it is accepted that professions do develop abstract, formal knowledge systems (explicit standing) from their first origins (Abbott, 1988, p. 57). Footing the concept of the security professional is the works of both Jaques (1989. P. 34) and Fox (1994, p. 203) which highlighted that in contrast to the implicit aspects of security's domain knowledge, professions are based on explicit knowledge, that which can be articulated. This is saliently important in the process of professionalisation, as professional education seeks out standardized educational criteria relating to such knowledge articulation. Such a requirement is because both the professions and their students need to be certain that they will learn the knowledge required to practice (Fox, 1994).

Much of the non-traditional societal security paradigm understandably sits within the criminological stream (Figure 2.2, Section 2.2), as criminals commit crimes against the state, persons, property, information and business reputations with the intent to gain advantage, do harm, or both (The American Architects Institute, 2004, p. 24). Smith and Brooks (2013, p. 2) consider that the best means to understand this paradigm is through the articulation of context or practice areas, highlighted through their applied domains (Table 3.1) (p. 17). Such domains arguably sit within the vast thematic or euphemistic categories of non-traditional security (Section 2.2.1).

Table 3.1 Hierarchical security domain subject categories of Brooks (2007)

Security domain subject category descriptors		
Criminology	Business Continuity Management (BCM)	Fire science
Facility management	Industrial security	Information & Computer
Investigations	Physical security	Security principles
Risk management	Safety	Security law
Security management	Security technology	

However, within the security domain there still lacks consensus of what constitutes the practice areas or contexts of security. For example, in contrast to Brooks' (2007) security domain subject categories (Table 3.1), ASIS International (2009, p. 16) offer their organisational version (Table 3.1).

Table 3.2 ASIS International Symposium Security Model (2009)

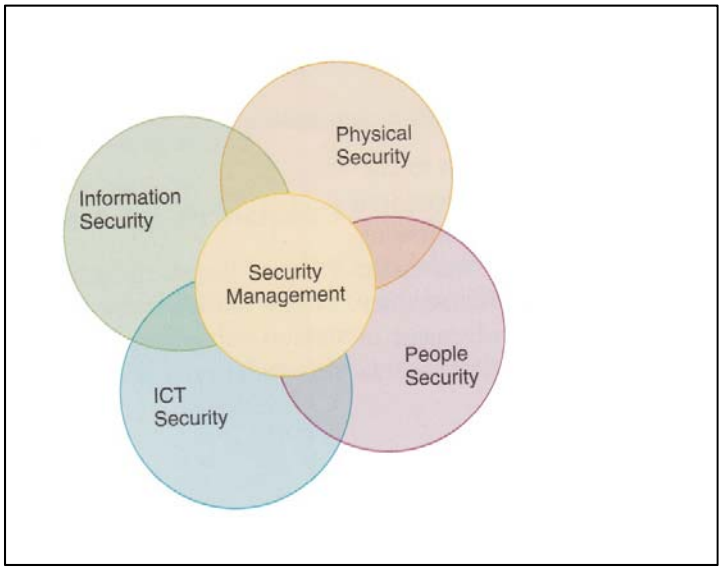
Physical Security	Investigations	Legal aspects
Crisis management	Competitive intelligence	Crime prevention
Personnel security	Loss prevention	Emergence/continuity planning
Disaster management	Executive protection	CPTED
Information security systems	Risk management	Fire protection
Counterterrorism	Violence in the workplace	Security architecture and Engineering

Nonetheless, both tables offer what can be considered knowledge categories and practice principles or areas inclusively, but without more focused depth or structure. This perhaps may be due to limited research and development into the structures of the greater discipline (see Smith & Brooks, 2013). In contrast again, Talbot and Jakeman (2009, p. 55) within their security risk management body of knowledge (SRMBOK) present five salient, overarching yet overlapping professional sets, or practice areas (see Figure 3.1) for contemporary security professionals. These are argued to sit across all of the non-traditional thematic categories of security. According to Talbot and Jakeman (2009, p. 55), the knowledge areas of security in this domain stream are to be centred on physical security, people security, the security of information communication systems

(ICT) and information security, layered over by the thematic category of security management (Figure 3.1) as another focussed domain area.

Accordant with Section 2.2, the combined literature introduces specific jurisdictional practice domains (Abbott, 1988, p. 2) for security and their potential knowledge content categories in relation to stored and indexed propositional knowledge (Sections 2.4 and 2.5). These practice domains and their underpinning propositional knowledge sit within and across thematic or euphemistic categories of security for those persons identified by the Australian Interim Security Professional's Task Force (2008, p. 6) as working at the senior end of the operational sector and in the strategic sector of the security industry.

Figure 3.1 Interrelationships of security practice areas (Talbot & Jakeman, 2009, p. 55)



While disparity reigns across the security discourse, in terms of knowledge area consensus, many authors offer a separated core jurisdictional field labelled Physical Security (Brooks, 2007, p. 5; Talbot & Jakeman, 2009, p. 55; ASIS, 2009, p. 3). Physical is defined as (1) relating to the body, as distinguished from the mind or spirit, (2) resembling material things or nature: the physical universe, (3) of or concerned with mater and energy, (4) of or relating to physics (Collins Dictionary, p. 972). Accordingly, the professional field or practice area of physical security is demarcated by ASIS International (2009, p. 3), Roper (1997, p. 1), Fennelly (2003, p. 101), Talbot and Jakeman (2009, p. 55) (Table 6), Baker and Benny (2013, p. 1) and Smith and Brooks (2013, p. 105) as that part of a security program concerned with physical control

measures designed to safeguard people, prevent unauthorised access to equipment, facilities, materials, documents, and to safeguard them against a security incident. Physical security measures include a device, system or practice of a tangible nature (Table 3.3) designed to protect people and prevent damage to, loss of, or unauthorised access to assets (2009, p. 3) utilizing a systematic approach (Garcia, 2006; 2008; Smith & Brooks, 2013).

Table 3.3 Talbot and Jakeman's security practice areas (2009)

Area	**Description**	**Activities**	**Practitioners**
Physical	Protection of physical assets as well as physical security measures designed to protect intangible assets or capabilities	Crime prevention through environmental design. Design and implementation of procedures and physical controls for protection of facilities, property, capabilities and physical aspects of ICT systems	Physical security advisers and consultants Guards, locksmiths, alarm and Closed Circuit Television (CCTV) installers and so on

Accordant with the study's denotation of security, physical security includes all those elements across the natural and built environment that are designed to reduce risk by controlling and managing geographical or spatial movement (Parker, 2007, p. 233). It is accepted that the best way to protect an asset is to control access to it (Coole, Corkill & Woodward, 2012, p. 28), or increase access difficulty (Kiszelewska & Coole, 2013, p. 28). In this context, The American Institute for Architects (2001, p. 6) emphasise that the major components of physical security employed in the built environment are access control, surveillance and response measures. Access controls aim to prevent unauthorised entry, and regulate authorised entry, into environments against those actions seeking to carry out hostile or illegal acts. Surveillance includes those measures to monitor and detect conditions that are, or potentially hazardous to people, information or property. The response component includes operational actions and procedures to intervene or neutralize a threat, or rescuing a victim, representing security algebraically as:

$$\text{Security}=\text{Access Control}+\text{Surveillance}+\text{Response}$$

In addition, The American Institute for Architects (2001) also consider that security should be driven by the threat, recognising that in contemporary times security, based on threat, may have to embrace enhanced strategies. These include mitigating against the effects of bomb blast threats (Building Hardening), or protection against biochemical threat concerns. In these circumstances an enhanced model of security is required, represented algebraically as:

Enhanced Security=

Access Control+

Surveillance+

Response+

Building Hardening+

Biochemical Protection

Such literature highlights that security is driven by a desire (philosophy) to protect against a threat, illuminated through risk messages and articulated through policy (cruciality). A physical security policy aims to direct environmental control or influence over an area. This aim is achieved through the process of using layers of physical manipulation measures, to mitigate against unauthorised access threats, or environmental design facets to reduce criminal opportunity within a location (Table 3.3) (Fennelly, 2003, p. 101).

Physical security layering defines the defensive elements of a facility in the three primary elements. These elements include the site and perimeter, the building envelope and the building interior, resulting in concentric defensive rings and zones (The American Institute of Architects, 2004, p. 44). These combine to prevent an unauthorised level of access to protected assets or inhibit opportunity through their material strength (Smith & Brooks, 2013, p. 105), design facets and practices to resist deviance. Such an approach is captured in Clarke's Situational Crime Prevention (SCP) framework (The American Institute of Architects, 2004, p. 45; Lab, 2013, pp. 216-219), which according to Kiszelewska and Coole, (2013, p. 28) provides a physical security rubric to reduce threat through increasing the difficulty, increasing surveillance and reducing the rewards. This approach is made possible through the integration of people,

procedures and equipment (Garcia, 2001; 2008, p. 1; Smith & Brooks, 2013, pp. 24-28). This field was also articulated as an essential sub-category within the embodiment of human security (Nef, 1999, p. 25) towards maintaining survival and the protection from sudden and hurtful disruptions in the patterns of daily life (Nef, 1999, p. 25; Roland, 2001, p. 89).

In considering the achievement of environmental control, a common or core theme that cuts across all domain categories of security is the concept of systems thinking. Therefore, salient within the physical security literature and of significance for defining a body of knowledge in this domain stream is the concept of systems thinking. As Underwood (1984, p. x) expressed, security should be designed, implemented and managed as a system. According to O'Shea and Awwad-Rafferty (2009, p. 14) such thinking is what affords an integrative, interdisciplinary, holistic perspective that builds parallel, complementary and interdependent aspects relative to security and the built environment. It is voiced in the writings of O'Shea and Awwad-Rafferty (2009, p. 14) that such an approach sees problems, including security problems, as part of an overall system.

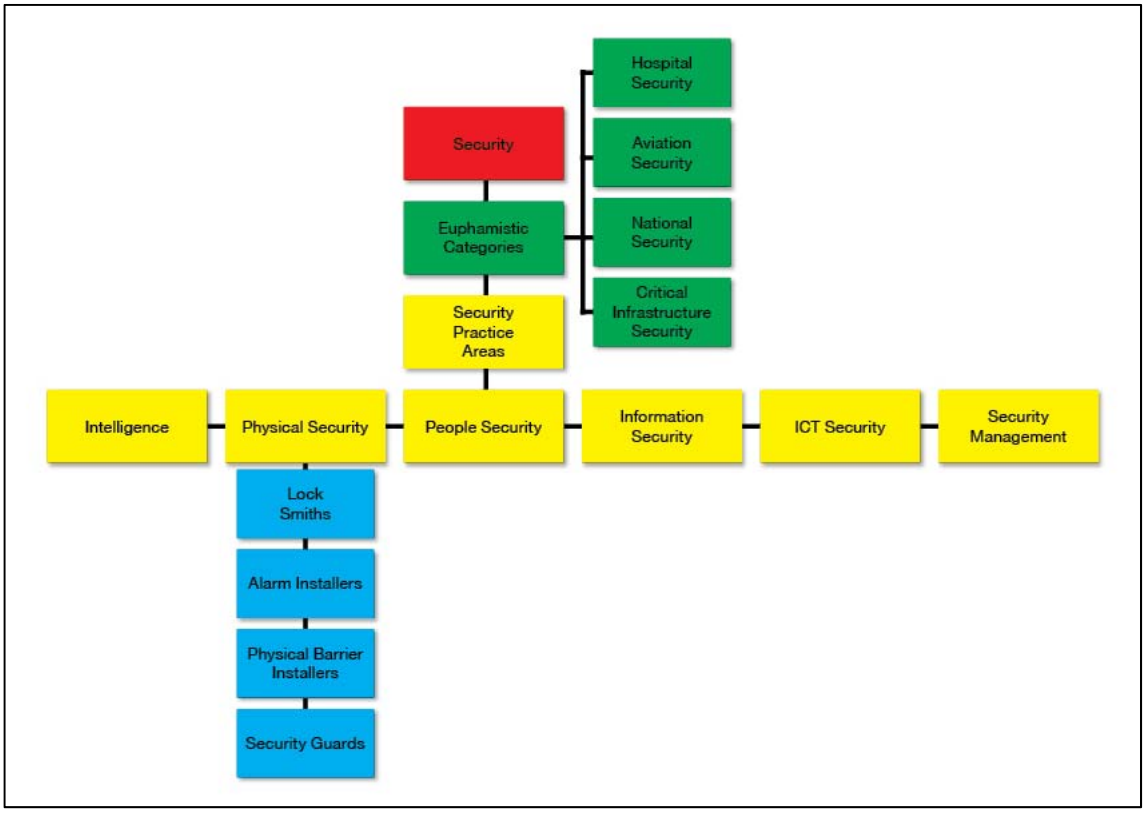
Within the security literature, Garcia (2001, p. 6) defined a system as an integrated collection of components or elements designed to achieve an objective according to plan. Where the plan for physical security is to interrupt or where necessary neutralize a malevolent adversary before they achieve their goal (Garcia, 2001; 2006; 2008). Thus physical security protects life, interests and property, which contribute to both survival and maintaining conditions of human existence across a vast array of protective contexts. As such, it is well acknowledged that this form of systematic security is considered to be the most fundamental aspect of any security program, which the reviewed literature highlights, transcends all security contexts, as Norman (2012, p. 94) states "all security begins with physical security".

Accordant with the earlier writings of Schnabolk (1983, p. 2), Manunta (1997, p. 21) reveals that functionally, evidence of physical mechanisms to control the environment such as physical access accompanies nearly every archaeological discovery. Locks, strong rooms, physical barriers and shields were known and used from the very beginning of civilisation. For instance, Schnabolk (1983, p. 228) points out that the first

recorded use of a lock that could be opened from the outside was in Egypt. Excavations of Egyptian tombs have disclosed locks that utilized an enormous key to move the locking device from side-to-side. In addition, walls, fences, and revetments of various kinds have long served as the first line of defence for specific sites. For example, the walls of ancient cities such as Troy, Jerusalem, and Jericho highlight how civilised worlds drew on physical modifications and barriers for protection against man (The American Institute of Architects, 2004, p. 4). Thus accordant with the study's narrative of security (Section 2.2.1) this accentuates the evolutionary processes within the domain category of physical security.

From its ancient origins (See Chapter 2) so embedded into contemporary life is physical security that regardless of security's diversity, Fennelly (2003, p. 101) and Norman (2012, p. 94), convey that all other security processes are integrated with physical measures to develop a contextual protection posture. Such depictions in principle support Talbot and Jakeman's (2009, p. 55) overlapping pose, and lead to the premise that physical security is not a euphemistic category, because it is a fundamental facet across all security contexts. Therefore as Schnabolk (p. 103), Fennelly (2003, p. 101), Brooks (2007), Talbot and Jakeman (2009, p. 55) Smith and Brooks (2013, p. 105) allude to (Tables, 3.1, 3.1, 3.3, Figure 3.1), physical security must be a salient jurisdictional knowledge category within the broader non-traditional professional domain of security. This articulation is represented indicatively through Figure 3.3, congruent with the writings of Wilson and Oyola-Yemaiel (2001, pp. 122-123) and Norman (2012, p. 364). As Norman clearly states, "there are different bodies of knowledge required for security system design, installation and maintenance. The skills necessary to be a great designer are different than the skills necessary to be a great installer, and that good designers, design to risk" (p. 364).

Figure 3.2 Indicative security domain taxonomy



Wilson and Oyola-Yemaiel (2001, pp. 122-123) explain that professions are occupations that have been able to establish specific jurisdiction over certain kinds of services. In reference to Figure 3.3, the concept of the physical security professional must be someone who sits overhead (vertical) of the trained occupational categories within the physical security set (Figure 1.1, Section 1.4). Supporting the premise that security professionals are bounded within jurisdictional foci accordant with other professions is the proposition put forward by Bloom. Bloom considered that expert versus novice research supports the premise that knowledge structures which make up proficiency in a given intellectual domain are distinctive to that domain (Anderson & Sosniak, 1994, p. 61). It is within this literature base that the assertion can be built that the jurisdictional depth and breadth of physical security as a professional domain category is not explicitly stated. That is, there is little consensus as to what constitutes the professional domain of physical security in terms of its knowledge content, structure and jurisdictional boundary for the modern day security professional rather than its allied practitioners (See Table 1.2, Section 1.3).

Such a poor state of articulation is disparate to Fox's (1994, p. 203) views, that educational criteria needs to be somewhat standardised. This means the knowledge and skills that individual physical security centred professionals require to perform their professional task of protecting their client's assets against incursions manifested through unauthorised access or crime facilitators is poorly defined. That is, it is not clear what a physical security professional is, or their knowledge and skills sets' required and its organisational structure to practice compared to that of other security professionals. For example, security managers accordant with boundary overlap, or allied practitioners such as technology installers or locksmiths (Table 1.2, Section 1.3 and Figures 1.1 and 3.3).

3.3 Professionals and the notion of jurisdictional boundary

The literature on professions highlights that the demarcation and distinction or jurisdictional boundaries in professional practice are of significant importance for professional standing and therefore for this study. Within this literature, Abbott (1988, p. 56) conveyed that "most importantly, any effective abstract system must explicitly define the borders of professional practice with utmost clarity". For this study, such demarcations or distinctions are specifically important between the often confused and overlapping knowledge categories or practice areas of Physical Security and Security Management (Figure 3.1).

Confusion arises, consistent with Norman's (2012, p. 94) remarks along with Talbot and Jakeman's (2009) views, that security managers, accordant with their own context, require knowledge of physical security practices, principles and measures. For instance, consistent with the writings of Bertalanffy (1968, p. 139), physical security systems are open systems as they attempt to achieve a steady state, but are affected by their internal and external environment (Coole, 2010; Smith & Brooks, 2013, p. 26) and therefore need to be managed as a system (Underwood, 1984, p. x; Coole, 2010, p. 226). Such management must be in-line with its original, or reviewed, design parameters (Coole, 2010, p. 226), or as stated by Underwood (1984, p. 250) be "managed by objectives". Thus, the professional design and management of physical security are often separate domain practice areas (See Figure 3.1).

Freidson highlighted that embedded in the claim of each profession is a paradigm, a taken for granted conception of what the issue is, and how it is solvable, where each profession views the world in terms of its own characteristic conception of problems and solutions (Freidson, 1973, p. 30). Therefore, a jurisdictional view resonates within the professions, where the reviewed literature (Section 2.7) considers, that in managing by objectives, Security Management embodies conceptual, administrative management, and security risk management arrangements; it is professional administration (Manunta, 1997, p. 54). In other words, security management can be considered within the systems approach of management, which accordant with the writings of Lussier (2009, p. 42), sees the organisation as a whole and as the interrelation of its constituent parts which are managed through interrelated tasks of planning, organising, staffing, leading, and controlling to achieve defined organisational objectives. This is a viewpoint congruent with the earlier demarcations established by Talbot and Jakeman (2009) (Figure 3.1; Table 3.1).

Within a jurisdictional purview, security management relates to the management of the means implemented to achieve security risk management, including technical, physical and procedural aspects, perhaps along with other jurisdictional categories (Figure 5). In contrast, physical security's jurisdictional foci are saliently focused towards establishing or implementing the necessary physical control measures (Table 6) to protect assets or prevent crime rather than its ongoing organisational management - the foci of security management. As pointed out by McNeil (1990, p. 73), definitions of how one discipline differs from another provides the organizational structure and indicates the borders of enquiry for that discipline. Such demarcation or boundary of professional practice is more clearly elucidated through the writings of Abbott (1988).

In affirming the distinction between physical security and security management, Abbott's (1988, p. 39) writings reveal the existence of several types of objective and subjective foundations for professional tasks that facilitate such jurisdictional division. According to Abbott some tasks are close together, where objective and subjective properties make problems alike, whereas others are further apart due to these very properties. Tasks that are objective are based within natural or technical imperatives, while those that are subjective are imposed by culture itself (1998, p. 36). In expressing that objective qualities lay in natural objects, facts and technological aspects, Abbott

(1988, pp. 39-40) offers the example that the body and the universe, water and weather, are objective aspects of the work of medicine, astronomy, hydrology and meteorology respectively. Whereas a profession's subjective aspects arise in the current construction of the problem by the profession, currently holding the jurisdiction of that task. Here Abbott refers to the concept of professional boundary accordant with technical knowledge and specific area of foci.

Abbott (1988, p. 40) conveys that in their cultural aspects, the jurisdictional claims that create these subjective or cultural qualities have three parts: claims to classify a problem, to reason about it, and to take action on it. Or, in more formal terms, to diagnose, to infer, and to treat an identified professional problem. According to Abbott (1988, p. 40), theoretically these are the three salient acts of professional jurisdictional practice. While professionals often run these modalities together, the sequence of diagnosis, inference and treatment embodies the essential cultural logic of professional practice. Abbott's (1988, pp. 36-41) writings highlight three salient sequential aspects of professionals' practice: the diagnosis, inference and treatment of target problems for their clients.

Abbott considers diagnosis as a means to assemble a client's needs into a picture and place this picture in the proper diagnostic category. In the security domain, the professional task of diagnosis is considered to be security risk management-an underpinning activity for all security practice (Talbot & Jakeman, 2009, pp. 134-134). Such a task is considered by Abbott as two interrelated processes, colligation (the linking of various isolated facts) and classification. Colligation means assembling the 'picture' of the client, consisting largely of rules declaring what kinds of evidence (Threat, Vulnerability and Consequences) (The American Institute of Architects, 2004; Talbot & Jakeman, 2009, p. 133; Standards Australia, HB167, 2009) are relevant and irrelevant, valid and invalid, as well as rules specifying the admissible level of ambiguity. Classification means referring the colligated picture to the dictionary of professional legitimate problems, ie. 'what they know'.

A classification system is a profession's own mapping of its jurisdiction, an internal dictionary embodying the professional dimensions of classification. Colligation is the first step in which the professional knowledge system begins to structure the observed

problems. Information passing through these rules is then assembled into a picture from a professional's long term working memory (See Sections, 2.2.3 and 2.3.3) that can then be classified (diagnosed). Abbott's (1988, pp. 41-49) work highlighted that information available to diagnose and reason about a problem may be incomplete or ambiguous at best. As such, there are likely to be several plausible accounts of the problem (colligations).

Abbott's (1988, pp. 41-49) views blend with the influential work of Jaques (1989, p. 24) who presents the issue of task complexity in professional work. Jaques emphasised two salient types of pathways for considering task complexity. Known pathways relate to those in which previously learned knowledge exists in available articulated form, and can be applied according to known rules, referred as retrieval from LTWM. In contrast, uncharted pathways are those in which there are unknown variables operating that create problems and call for the continual exercise of discretion, judgement and choice making. The art of diagnosis therefore lies in finding the real issue. Therefore, within the three aspects of professional practice is the distinction between well-defined, medium-defined and ill-defined problems (Eraut, 1994, p. 45).

According to Eraut (1994, p. 45) for a problem to be well-defined there must be one clearly preferable solution and a small change in the problem results in a small change in the solution. However, where more than one potentially acceptable solution exists, the problem is considered "moderately-defined". In either of such cases, there is wide consensus concerning the range of differential diagnosis and treatments and principles underlying their solution. Conversely, with ill-defined problems there may not be an ideal solution, or there may be more than one solution where small changes in the problem require large changes in the solution. In such an instance, professional problem solving strategies are required (Eraut, 1994, p. 45). According to Jaques (1989, p. 34) for complex problem solving it is the exercising of judgement and making decisions that you pay professionals for.

Abbott's (1988, p. 49) work emphasized that a profession's diagnostic classification system is organised as a probabilistic hierarchy from common to esoteric rather than from general to specific. In the security context, this is explained as "the security assessment process works from the more obvious to the less obvious threats (The

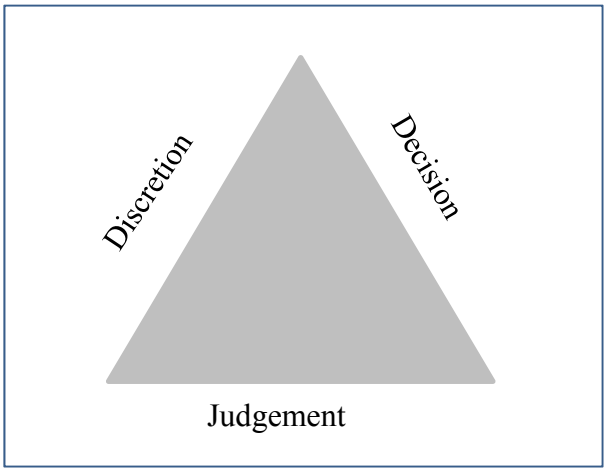
American Institute of Architects, 2004, p. 34) and treatments". In addition, where costs of failure are low and the professional is assured of a second chance, the most likely treatment is prescribed. This results in a short diagnosis-treatment time structure. But where the outcomes are prohibitive (high costs), or there is no second chance, a professional must set a strategy for treatment from the outset, through means of professional inference. This is undertaken when the connection between diagnosis and treatment is obscure, that is, a more ill-defined problem. Abbott (1988, p. 49) states:

> Professional inference can work by exclusion or by construction. For example, medicine, when a case is unclear, works by exclusion where doctors maintain a general supportive treatment while ruling out areas by using special diagnostic procedures, or watching the outcomes of 'diagnostic' treatments provided, beyond general maintenance.
>
> In contrast, classical military tactics work by construction. Here the tactician hypothesizes enemy responses to gambits and considers their impact on his further plans. Here a tactician, due to the somewhat limitations in an adversary's responses, constructs a plan allowing as many wining scenarios as possible, or those which may not win, but do not lose...where the emphasis is on constructing possible battles ahead of time, rather than fighting little ones to find out what does not work. (Abbott, 1988, p.49)

Such an articulation indicates that reasoning by exclusion is a luxury available only to those who frequently get a second chance (sometimes not the case in the security domain). Thus, Eraut (1994, pp. 48-50) suggests that professional problem solving knowledge may get used in four modes. It may be used in a replicative mode, characterised by the close similarity between the epistemological context in which the knowledge was acquired and rehearsed (specific transfer) and that in which it is used. Alternatively it can be used applicatively, in a setting in which circumstances are unique or different from that of replicative mode (non-specific). On the other hand, interpretative use of knowledge involves the more mysterious quality of professional knowledge, and is referred to as 'professional judgement' embodying practical wisdom and feasibility along with appropriateness (discretion, judgement and choice making).

Professional judgement introduces the intuitive, more implicit aspects of knowledge use and includes the use of associative knowledge. Associative knowledge draws on knowledge presented in images or heuristics to employ knowledge principles (Eraut, 1994, pp. 48-50) to solve ambiguous professional problems (non-specific transfer). Jaques (1989) represents this process through a tripartite cognitive model, which sees the outcome of problem solving (reasoning-inference) as an interrelationship between the elements of judgement, discretion and decision (Figure 3.3).

Figure 3.3 Cognitive processes trio for professional complex problem solving



Abbott's (1988, p. 49), Jaques (1989) and Eraut's (1994) views are congruent with the writings of Clarke (1992, p. 5) and Garcia (2008, p. xvii), and the views of the Advancing Security Professionals Congress, which highlighted that one hallmark of security professionals is their capacity to break new ground in an informed and responsible way (p. 9) (inference). Drawing on the writings of Abbott (1988), Jaques (1989), Clarke (1992, p. 5), Eraut (1994) and Garcia (2008), the study is focused towards the objective qualities of the physical security domain or practice area (the science and learning's) as they lie in the subjective qualities (cultural jurisdiction) of diagnosis, inference and treatment. These combined qualities embody the four problem solving modes of replicative, applicative, interpretative and associative principles towards physical control concerns. Such concerns incorporate primary and secondary crime prevention strategies within the tripartite crime prevention model against a constructed or exclusionary threat, thus, the security risk context.

The tripartite model of crime prevention sees strategies categorised according to their intervention focus (Lab, 2013, p. 28). Primary crime prevention focuses on physical and procedural measures designed to take effect before a crime occurs or offenders are identified, to reduce opportunities for potential offenders to engage in deviant acts. This includes neighbourhood watch and the use of private security, along with environmental design techniques. Environmental design focuses towards establishing a higher level of difficulty to commit a deviant act and may include situational measures such as surveillance, lighting and locks, fencing, along with property marking techniques that enables a level of control to be exerted over an area. Secondary prevention also focuses towards situational and social strategies but is steered towards existing problems, and tailors situational and social strategies towards highly specific deviances accordant with the crime problem (Lab, 2013, pp. 28-29). Lab (2013, p. 29) explains that the distinction between primary and secondary crime prevention lies in the contextual focus at the time, as many secondary efforts resemble those of primary prevention. Primary prevention aims to prevent the conditions that foster crime from arising (deterrence), whereas secondary prevention efforts are focused towards factors that already exist and are fostering deviance (treatment).

O'Shea and Awwad-Rafferty (2009, p. 22) expressed that for the purposes of protective design (primary and secondary crime prevention), security is focused towards the protection of assets, both physical and psychological from unauthorised access, theft and damage. They consider the goal to be the deterrence or the detection and apprehension of offenders, focusing towards prevention. The American Architects Institute (2004, p. 13) supports this view expressing the general goal of physical security is the protection of assets by providing enough time during a security event to facilitate a response. Accordingly, the reviewed literature jurisdictionally presents physical security as the use of physical and technological measures combined with procedural processes (Fennelly, 2003, p. 101) that as integrated systematic components provide environmental control or a level of difficulty to overcome for both opportunistic and planned adversaries.

Such measures contribute to securing an environment utilizing technical, physical and procedural control variables integrated into a barrier system and defined as a Physical Protection System (PPS) (Garcia, 2008, p. 5; Smith & Brooks, 2013). In contrast, while

significant overlaps exist culturally (Talbot & Jakeman, 2009, p. 55), security management relates to the diagnosis, inference and treatment of management concerns as they relate to achieving organisational objectives utilizing the security function. Security management is saliently focused towards management acts including planning, organising, staffing, training, leading and controlling, along with budgeting where physical security forms a component of a broader cultural posture.

The combined literature highlights that for the professional tasks of diagnosis, inference and treatment of societal problems, within the domain of physical security, a PPS is achieved through layers (O'Shea & Awwad-Rafferty, 2009, p. 247) of technical, physical and procedural control measures (Smith & Brooks, 2013) as a treatment strategy. These measures are directed at protecting an environment or asset (Corkill & Coole, 2013) through deterring, removing opportunity or preventing physical access (Fennelly, 2003, p. 101). In addition, where unauthorized access is gained or opportunity exploited, physical security facilitates detection, delay and response within a defined period of time with resilience against a defined threat actor's actions (Garcia, 2008, p. 5; Smith & Brooks, 2013).

Thus, consistent with the writings of Wolfers (1952), Schnabolk (1983), Abbott (1988), Clarke (1992, p. 5), Manunta (1997), O'Shea and Awwad-Rafferty (2009), Talbot and Jakeman (2009) and Smith and Brook's (2013) works, physical security as professional jurisdictional foci is directed towards the diagnosis, inference and treatment system of security or loss coupled risk concerns manifested through unlawful access or crime enablers in the protection of assets. Loss or risk concerns include threats to people, information and property, where treatment is synonymous with control and is pursued accordant with the economic law of diminishing returns (See Section 2.2.1). A point emphasised by the American Institute of Architects (2004, pp. 12-19) text, highlighting that as with the earlier writings of Wolfers, a balance between physical security measures and budget must be achieved, stating "all security decisions involve long-term cost considerations, with respect to operating personnel and systems, as well as maintenance and repair". Such systematic treatment results in a security function as an organised complex of specialised technological, physical and procedural elements integrated into a protective barrier system.

Informing the idea of a professional body of knowledge for physical security professionals, the reviewed literature emphasises that physical security should be integrated as a system. Such a system achieves a desired level of control within a context (Corkill & Coole, 2013, p. 144), based on sound methodology. Congruous with the writings of Fox (1994, p. 202), Freckelton and Selby (2013, p. 1051) and Smith and Brooks (2013, p. 1) such a systematic approach should comply with well-identified theories, principles, means and methods, as a knowledge structure based on the science or learning on which they are founded. As such, the jurisdictional framing or boundary of enquiry for this study must lie in the cultural demarcation relating to organised, stored and indexed declarative-propositional knowledge.

This knowledge relates to the skills embodied within diagnosis; inference and treatment of those physical protection or primary and secondary crime and prevention concerns manifested through opportunity, crime facilitators, or unauthorized access of an area or space. Whereas a jurisdictional foci, physical security aims to implement control measures in a delineated environment to mitigate the risks associated with an expressed threat. Such expression is the articulated diagnosis of the problem achieved through security risk management.

3.4 Defining a profession accordant with its body of knowledge

The reviewed literature highlights that diagnosis inference (reasoning about) and treatment are aspects of professional practice accordant with the science or societal learning that underpins their jurisdictional application. Such learning exists within the four problem solving modes, accordant with their objective and subjective professional properties. According to Abbott (1988, p. 52), in most professions these aspects are tied directly to a formal system of knowledge that formalizes the skills in which this work proceeds. Thus, accordant with the reviewed works of Abbott (1988, pp. 52-54; Wilensky, 1964; Eraut, 1994; Griffiths, Brooks & Corkill, 2011; Freckelton & Selby, 2013) academic knowledge legitimizes professional work. Academic knowledge clarifies professional foundations, tracing them to major cultural values, where in most modern professions these have been the values of rationality, logic, and science, where academic professionals demonstrate this rigour (Abbott, 1988, p. 54).

It is emphasised within the reviewed literature that historically medicine has been held up as a codified knowledge benchmark by society in formal bodies of knowledge discourses (Wilensky, 1964; Abbott, 1988). As with security's historical roots; the practice of medicine existed in early cultures, where the Greeks pursued a distinctly natural rather than supernatural approach (Freidson, 1970, p. 13). However, unlike security practices, according to Freidson (1970), the Hippocratic physicians accentuated an objective approach, systematically codifying knowledge through careful observation and description of diseases and their cause, with a view to accurate prognosis and ultimately treatment. For example, in Greek and Hellenistic times, formal schools participated in describing and classifying disease, organs and biological processes (codification), with seven hundred years of medicine, beginning with Hippocratics and ending with Galen in which a number of observed recordings were documented that are still considered correct in contemporary times. This development included careful anatomical descriptions of the eye, the trachea, the duodenum, together with descriptions of diabetes, leprosy and tetanus (Freidson, 1970, pp. 13-14), supporting the efficacy of meticulous codification in preparation of later transmission.

Medical knowledge codification was further enhanced in the seventeenth and eighteenth centuries through further medical observations and developments. However, the development of both physics and chemistry as academic domains made possible a more robust systematic foundation for contemporary medicine. Freidson (1970, pp. 14-15) contends that without such a foundation medicine as a profession would not be more than a variety of traditional conceptions, supplemented by quite variable individual clinical judgements, arguably where physical security seats currently. These developments were supplemented by technological advances in anaesthesia and parallel developments of a sociological foundation to create an occupation well established in society; a group "in command of the formal criteria that qualify men to work at healing, of exclusive competence to determine the proper content and effective method of performing medical work, and freely consulted by those thought to need its help" (cruciality) (Freidson, 1970, pp. 16-17).

Congruous with the writings of Wilensky (1964), Freidson (1970, p.338) states: "we can justify removing decisions from the hands of the layman and placing them in the hands

of experts when only the experts have the especially reliable knowledge by which to make correct decisions in the lay interest (mystique)".

Thus, in the medical profession, Freidson (1998, p. 338) considers a professional to be an expert because he or she is trusted to possess some special knowledge unavailable to the laymen (mystique), who have gone through their special standardised course of professional training. In addition, it is recognised that such professional knowledge may not be demonstrably and consistently efficacious, but it is the best available to the times, and it is taught to all members of the profession in order to prepare them for proper performance of their work. The referents of 'knowledge' and 'expertise' refer to a body of assumed facts ordered by some abstract ideas and theories that are applied to a level that instils public trust in solicited services. These putative facts are embodied in the treatises and textbooks that provide the formal substance of what experts learn in professional schools and what they presumably know thereafter.

The reviewed literature highlights that the academic-abstract knowledge system is arguably universally important throughout the professions, where "a profession's ability to sustain its jurisdiction lies partly in the power and prestige (evaluative) of its academic knowledge (cognitive)" (Abbott, 1988, pp. 54-55; Martin & Guerin, 2005, p. viii). Therefore, the professional seating of the study lies in elucidating a formal system of knowledge for physical security professionals, defined as the abstract knowledge needed by these practitioners to perform their profession's work (Martin & Guerin, 2005, p. viii) and invoke professional trust. Such a resource is considered a "professional's formal knowledge system" (Abbott, 1988, p. 53) which can be standardised and taught to all future members regardless of their place or institution of education.

As such, central to the study's discourse is the argument put forward by various authors including Martin and Guerin (2005, p. 16; Abbott, 1988, pp. 54-55; Eraut, 1994, p. 45) that a body of knowledge defines a profession's jurisdictional practice. This view is also supported by Morris, Crawford, Hodgson, Shepherd and Thomas (2006, p. 710) who assert that ownership of a distinctive body of knowledge is a vitally important element of a profession. This very viewpoint is also promoted in the literature of Epstein and Hundert (2002, p. 227) who expressed that dimensions of professional competence

include a cognitive component-acquiring and using knowledge to solve problems, underpinned by other core facets. Gillespie (1981, pp. 17-18) claimed that while it is difficult to build systematic bodies of knowledge and theory within cohesive and well-defined professions, within diffused professions (security) this task is more difficult, but nonetheless achievable.

3.5 Professional status within the security domain

The emerging theme is that a recognised professional in the societal group phenomenon is a person who holds special jurisdictional knowledge based within a systematic foundation passed on through formal education, that is taught to all category members. The reviewed literature therefore leads to the assertion that the security profession as a broader domain reflects a more taxonomy of occupations of specialized jurisdictional foci supported by declarative-propositional knowledge both as generalized and context specific. This literature highlights that if security, and more specifically physical security, is to achieve recognised professional status (profession) there exists a crucial need to explore and establish its jurisdictional academic knowledge content, structure, skills base and ultimately educational requisites. Such an investigation will inaugurate external credibility for the domain and its educational necessity. Such an explicit view has been emphasised by varied writers within the security domain including Tynjala (1999), Garcia (2000) and Smith and Brooks (2013).

For instance, Tynjala (1999, p. 373) conveyed that more transferable knowledge needs to be produced for security practitioners using instructional methods that support understanding, emphasise application, and integrate theoretical and practical knowledge. Accordingly, Garcia asserts that as with disciplines such as medicine and psychology, practices within the security industry should be driven by research and validated results (2000, p. 80), which arguably can only be achieved through formal knowledge codification. Therefore, accordant with the writings of Wilensky (1964), Abbott (1988), Eraut (1994), Garcia (2000) and Smith and Brooks (2013) for security practitioners at the senior end of the operational sector and within the strategic sector (See Advancing Security Professionals Task Force, 2008, p. 4) to be viewed as professionals in the group phenomenon it is essential that accordant with a scientific or

constructed model basis for the profession, higher education needs to formally identify their core knowledge base.

Furthermore, adequate representation of the domain's knowledge content is essential for developing a validated curriculum and assessing professional proficiency to gain public support, trust and ultimately professional status. Here the writings of Bruner (1977, p. 2) highlight that adequate representation not only includes content but also structure and connections, congruous with the premises underpinning cognitive constructivism (Section 1. 6). For example, according to Bruner (1977, p. 8) scientists constructing curricula for physics and mathematics have been highly mindful of, and that their early gained success has been due to, the emphasis of teaching knowledge structure. Therefore, the driver to establish academia as the vehicle for steering recognition of the security professional, and specifically a physical security professional, is supported by the idea that the university is the focal point of professionalism (Gillespie, 1981, p. 371).

Higher education institutions are based on maps of propositional (factual) knowledge that they use for the construction of a syllabus (Eraut, 1994, p. 103). For example, the observed differences between experts and novices suggest that student proficiency can best be increased by instruction that facilitates the construction of knowledge bases that are comprehensive, structured in terms of higher-order principles and inclusive of problem-solving procedures. These knowledge bases can be supported by cognitive structures such as heuristics along with specifications of the conditions of their applicability, and framed by appreciation of the distinctive goals of the domain (Anderson & Sosniak, 1994, p. 61). The term heuristic is of Greek origin, and means, serving to find out or discover (Gigerenzer & Gaissmaier, 2011, p. 454). Heuristics are considered mental shortcuts (Weiten, 2002, p. 251), developed to simplify and reduce efforts associated with a task (Shah & Oppenheimer, 2008, p. 207). They represent both a conscious and unconscious cognitive process (Gigerenzer & Gaissmaier, 2011, p. 451) developed to aid and enhances efficient judgements surrounding a topic of foci (Shah & Oppenheimer, 2008, p. 207). Such a cognitive short cut allows the brain to create links and store conceptual information frames in a meaningful way, enhancing memory and retention of information (All, Huycke & Fischer, 2003). Gigerenzer and Gaissmaier note that Einstein included the term (heuristic) in his Nobel prize-winning paper,

indicating that the view he presented on quantum physics was incomplete but highly useful.

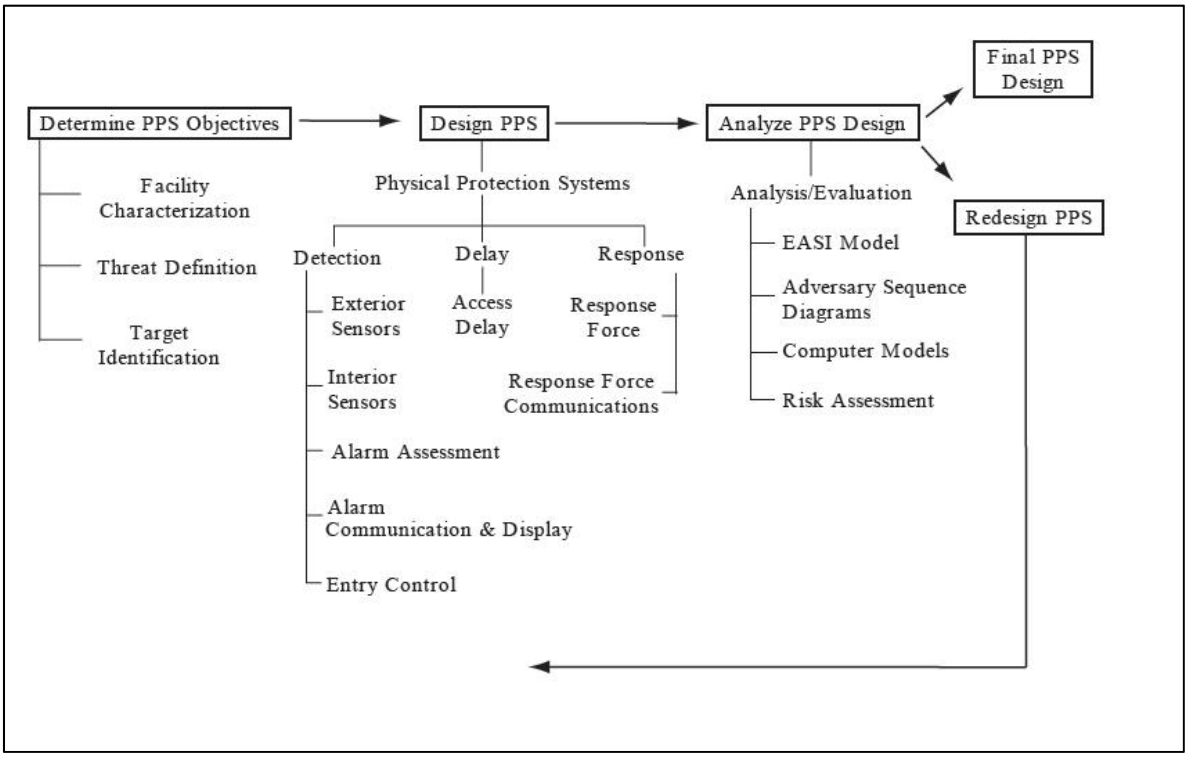
The works of Dhami and Harries (2009), Keller, Cokely, Konstantinos and Wegwarth (2010) and Marewski and Gigerenzer (2012) highlight that heuristics are widely used in contemporary society to help represent conceptual information in a meaningful way. In education the use of concept map heuristics in the form of spider maps, hierarchy maps, flowcharts and system maps have been shown to aid students with learning, understanding, recalling and integrating information (All, Huycke & Fischer, 2003; Bes Pia, Blasco-Tamarit & Munzo-Portero, 2011; Daley & Torre, 2010). Such reception learning builds declarative memory (Goucher, 2009). In their review of studies on decisions by individuals and institutions, including business, medical and legal decision-making, Gigerenzer and Gaissmaier found that decisions based on heuristics can often be more accurate than more complex 'rational' strategies (2011, p. 473) and they save effort (p. 451). Thus, a vast body of literature supports the use of cognitive tools or heuristics for understanding and imparting knowledge structure.

In the educational environment, the work of All, Huycke and Fischer (2003, p. 311) highlighted that the ability to put information together in meaningful ways improves retention of that information as well as understanding. They express storage of information in a manner that facilitates meaning is a cognitive process that promotes the act of remembering. The work of Fraser (1993, p. 24) explained that such cognitive structures could consist of a number of areas of knowledge, each a distinct knowledge domain. Each of these knowledge domains encapsulates a different area of knowledge. In this context learning is an interactive process where learners form linkages between newly perceived information and the previously created knowledge of the subsumer (p. 27). Fraser states:

> The construction of relationships between concepts enhances the meaning of each of the interrelated concepts. Similarly, the enhancement of the meaning of one concept in a conceptual framework serves to enrich the meaning of other concepts within that framework. (Fraser, 1993, p. 27)

The work of All, Huycke and Fischer (2003, p. 312) asserted that key factors which are associated with meaningful learning include: 1) assimilation of new concepts and propositions into existing cognitive structures, 2) knowledge organised hierarchically in cognitive structures, and 3) subsumption of concepts and propositions into existing hierarchies. Accordingly, professional knowledge domain heuristics can be considered 'rules of thumb' for understanding the individual knowledge areas, their significance, along with presenting in simplistic form how they integrate. They aid in educational comprehension, and highlight how specialized knowledge can be applied to problem solving, serving as varied maps of propositional knowledge. For example, Garcia (2001, p. 4) drew on a heuristic representation to show how for a physical protection system (PPS), the system elements are linked together to achieve the system's goals (Figure 3.4). Figure 3.4 has become a domain heuristic for understanding relationships within the design and evaluation of PPS. Accordingly, heuristics can and are used to effectively communicate knowledge and structural relationships within a domain area of interest.

Figure 3.4 Garcia's PPS design and evaluation heuristic



The complexity of professional learning means that it is within the university that the initial training and preparation (professional education) occurs prior to entry into the professions (Gillespie, 1981, p. 372). The work of Eraut (1994, p. 103) divided professional knowledge into three salient categories including (1) discipline based theories and concepts derived from bodies of coherent, systematic knowledge, (2) generalizations and practical principles in the applied field of professional action, and (3) specific propositions about particular cases, decisions and actions. In such institutions professional knowledge is taught as the tool to diagnose, infer and treat (Abbott, 1988, pp. 36-41) problems in one of four modes, replication, application, interpretation or association (Eraut, 1994, p. 103).

In examining higher education for security professionals, the work of Ericsson and Charness (1997, p. 34) highlighted that the broad literature of expertise suggests that human expertise involves two complementary processes (1) a high motivation to put in hours of deliberate practice necessary to acquire the mechanisms to bypass human physical and cognitive limitations, and (2) acquire the knowledge base necessary to respond accurately and flexibility to the tens of thousands of unique cases an expert may encounter. While engaging in hours of study is an individual endeavour, higher educational research can contribute to the means in which students can more efficiently and effectually acquire the knowledge base necessary for dynamic practice. For this element of higher education, Sternberg (1997, p. 153) points out that educationally it is the organization-of-knowledge that is of dominant importance, as "one has to know how to organize what one knows". Accordingly, Feigenbaum (1985, cited in LaFrance, 1997, p. 168) considered that expertise is something that has to be captured with an educational goal, to capture and incorporate the domain expert's fundamental knowledge into existing knowledge structures .

Today a formal pattern of professionalisation exists in society, so that now a major credential for the acceptance of a new applied profession is the acceptance of its program within the university framework (Gillespie, 1981, p. 372). Cogan's (1955, p. 108) early work implied this view, stating, "it is very necessary to set up standards (definitions) for accredited schools: their admission requirements, their formal curriculum, along with formal qualifications of instructional staffs and the requisite facilities for its instruction". Focusing on the curriculum component of professionalism,

consistent with the writings of Fox, (1994) a critical role for higher education is to define the security profession and provide the academic learning base that allows the establishment of generalised standards and credentials underpinning the breadth and depth the security domain (Rogers, 2000, p. 65) and supports the classification of security professionals as a cultural group.

3.6 The ambiguity of security education

In looking towards the future, Freidson (p. 27) in 1973 wrote that it was accepted by most futurologists that the projected outlook for society sees an ever-increasing reliance on specialized knowledge and skill, and on applying this knowledge to the solution of practical problems by specially trained individuals. Such a view may explain the many emerging professions within modern society such as interior design, safety or human resource management. However, professionalisation for security is proving difficult due to poor understanding of the domain space. For instance, it has become a well-acknowledged theme within the reviewed literature that security's contemporary knowledge base is poorly defined and as such, its educational goals and standards are sporadic at best, consequently refuting the very concept of the security professional as a group phenomenon in possession of consistent specialized knowledge and skill. Rogers (2000, p. 66) stated that the challenge for supporting the security professional as an occupational group lies in defining the common threads that bind security's domain diverseness together from the broadest possible perspective, that is the general as well as the specific. However, neither is undoubtedly articulated.

Brooks expressed the view that there have been research attempts to achieve this through defining a security body of knowledge, but with limited agreed consensus (2007, p. 1). As Borodzicz and Gibson (2006, p. 189) point out, there exists much controversy surrounding the choice of a security curriculum, as some argue security is fundamentally an area of criminology. Yet the strategic corporate level is more a management science, consequently clear jurisdictional boundary is essential. Furthermore, attempts to define security professionals according to educational qualifications are compounded by the truth that regardless of the paucity of an accepted body of knowledge, since September 2001 there has been a proliferation of programs offering courses, certificates and degrees in security or homeland security. Yet these

courses have no vetting process to determine the quality or legitimacy of the conferred credentials (Rogers, et al, 2007, p. 2) and offer what Brooks (2007, p. 2) contends to be allied discipline education badged as security education.

Nevertheless, Ericsson and Charness (1994, p. 738) stress that a relative uncontroversial assertion is that training to an expert level of performance in a domain requires mastery of all the relevant knowledge and prerequisite skills. Such a point highlights the very problem for security professionals as a group phenomenon. That is, the study of security at the university level is recognised to be disparate, drawing on a broad unfocused body of knowledge (Table 1). This knowledge incorporates a vast array of theory and principles across multiple areas of foci, across multiple domain disciplines, without a clear professional and supporting educational objective. In addition, outside of the profession's discourse (Section 2.2.2), there does not exist literature or governing body requisites that overwhelmingly state that a security professional must attain a university qualification. Nor do registration regulations exist requiring this, with most requisites focusing towards the occupational sectors (See Table 1.2 & Figure 1.1) and their associated licencing such as installers and maintainers. For instance, in the West Australian context, police licences require a Certificate four in Security and Risk Management, or higher to become a security consultant. However, in-house security advisors do not require this. A critical analysis of such training courses highlights a lack of core security knowledge, supporting the view that educators at this level do not know what to teach.

Phinney and Smith (2009, p. 2) support these broad criticisms which undermine the professions stream of the security domain, highlighting that the knowledge domains of security science are relatively unknown. Consequently, this acknowledgement arguably challenges the very requirement for security focused university education. In addition, for practitioners, especially physical security specialists, not all theories and principles across its broad domains are directly relevant within their jurisdictional foci (subjective properties). Consequently, there are no universally accepted learning objectives and supporting knowledge base to draw curriculum and assessment instruments from for the professions stream of the security domain.

3.7 A higher education curriculum for security science

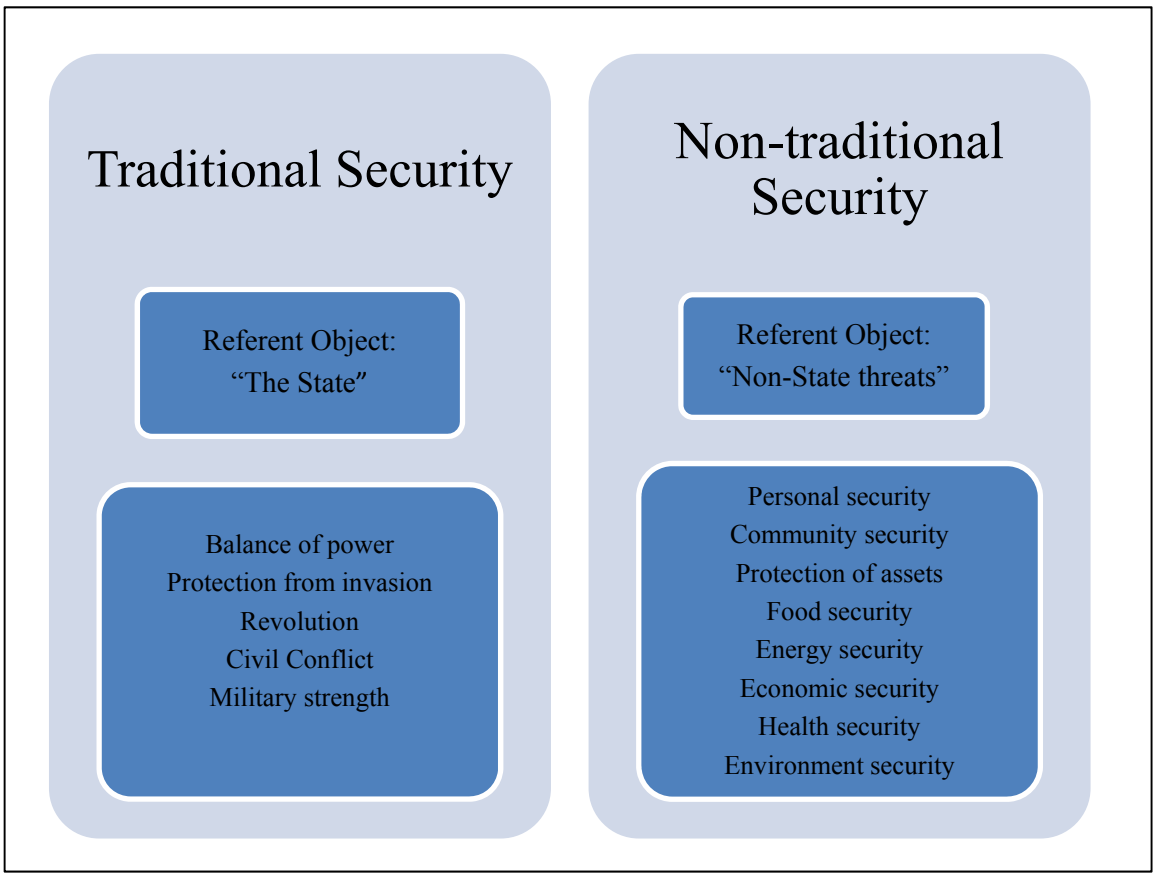
The concept of a formal professional stream based on the sciences and learning that underpins the concept of security within the non-traditional domain of security is perhaps new by historical standards. However, the non-traditional domain of security is saliently centred towards the notion of crime prevention, and within this contemporary notion exist disparate domain jurisdictional views. For instance, towards the notion of crime prevention within society Lab (2014, p. 32) refers to the emerging domain of crime science within the crime prevention realm, yet Smith and Brooks (2013, p. 21) refer to the contemporary professional domain of security science. For instance, drawing on Laycock's (2005) work, Lab explains that crime science as an emerging discipline relates to the application of the methods of science to the problem of crime and disorder.

According to Lab (2014), the emerging discipline of crime science focuses on attacking crime in society utilizing a wide range of disciplines, employing a broad array of tools to control or manipulate the social and physical environment in the fight against crime. This approach includes the development of safety and security devices, or a myriad of other factors that play a role in crime and crime control. Smith and Brooks (2013, p. 21) articulate the notion of security science in a similar manner, defining it as "an emerging academic discipline that brings together broader discipline concepts into a structured body of knowledge, integrating them into a single domain boundary". This theme is repeated for the domain of crime science, which is purported to include the disciplines of sociology, psychology, criminology, engineering, physics, architecture, computer science, biology, genetics, communications and education. It is stated that the primary goal of crime science is to bring these diverse disciplines together into a functional, coordinated response to crime (Laycock, 2005). But this articulation puts emphasis on law enforcement functionalities as well.

Nevertheless, the United States Hall Crest Report (1985, p. 225) formally acknowledged that while security and law enforcement comprise overlapping ideologies, they are distinct knowledge domains. Not incongruent with the notion of crime science, Smith and Brook's (2013, p. 21) definition of security science emphasises a domain boundary which includes overarching knowledge areas of security management, security theories and principles, the built environment, and security risk management. They also include knowledge areas of physical security, personnel security, industrial security and business continuity management. They consider that such principles may include the functions of deter, detect, delay, response and recover to criminological concerns.

This combined literature presents an argument for a recognised branch of formal learning jurisdictionally separate from international relations (Traditional security) that requires action based on the sciences and learning to resolve crime or security related problems in society. In addition, while the concept of crime science cannot be snubbed, the focus of this study is towards the sub-domain or practice area of physical security. As such, the emphasis is towards informing a body of knowledge for physical security professionals. Therefore the study will draw on the notion of security science as opposed to crime science to further seat its investigation. Such reviewed literature bares the supposition that Security Science (Smith & Brooks, 2012, pp. 2-3) as opposed to international relations (Section 2.2.1) as a professional focus is a branch of contemporary science underpinned by codified scientific knowledge relating to the built environment, the protection of assets and crime prevention within the non-traditional domain of security. This discourse highlights two broad sub-domains of security as an academic discipline, where physical security is arguably a further sub-domain within the broader non-traditional domain of security.

Figure 3.5 The two salient domains of security

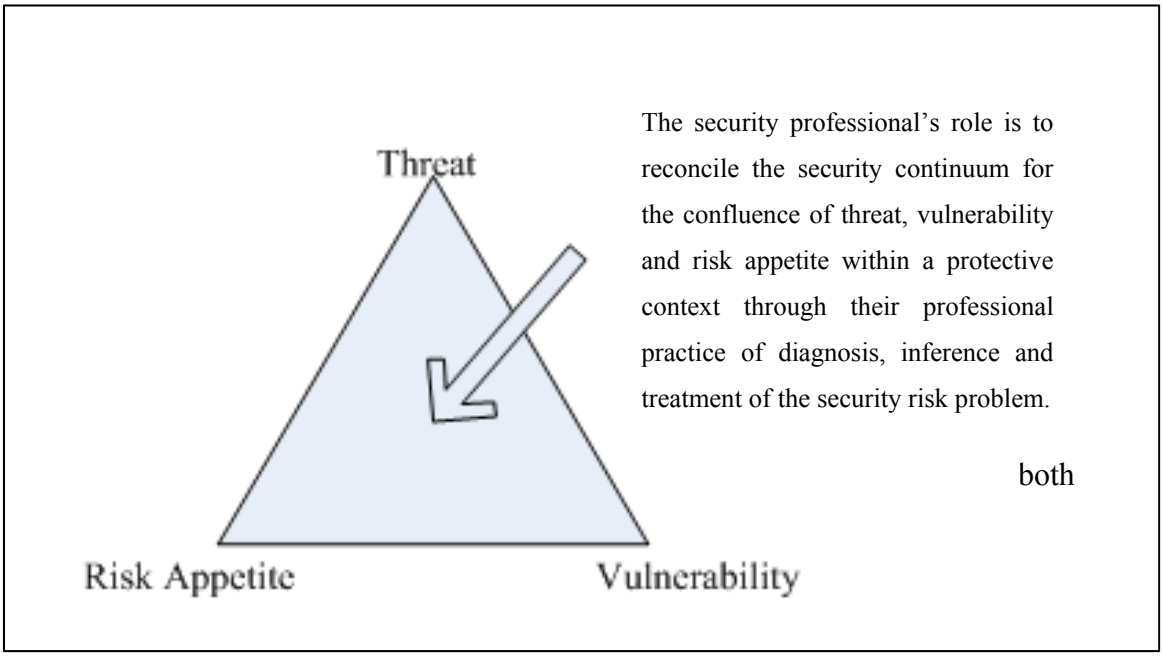


Accordingly, the status of the security professional in this domain stream must relate to somebody formally educated in the means of diagnosis and reasoning about society's protective security and crime prevention problems. Then applying validated techniques from this branch of knowledge to solve such problems at a professional level. That is, to reconcile the types and levels of control in relation to a confluence of threat, vulnerability and consequences through underscorings of risk articulation (Figure 3.6) for a protected value or asset. Congruent with the writings of Freidson (1970, pp. 14-15), the necessary developments in the areas of physics, electronics, criminology theory, psychology and architecture, along with many more disciplines has made possible a systematic foundation (Section 2.4.1) for the development of a formal physical security professional's body of knowledge.

The reviewed work of Mosher (1968, p. 106) exclaimed, "a profession is an unambiguous occupational field, which requires higher education". Therefore, as emphasized within the literature, central to security's profession-professional discourse

as a group phenomenon is a curriculum linked directly to a consensual body of knowledge. This knowledge is organised in a systematic manner, according to its jurisdictionally verified knowledge base of the science and learning on which it is founded, framed within the goals and objectives of the profession.

Figure 3.6 Non-traditional security professionals' foci



Congruent with this articulation, the works of Fox (1994, p. 202) convey that both prospective professionals and the public rely on uniform standards of education. Such standards develop dependable expectations regarding the scope of any profession and the competencies that those who complete its formal education can reasonably be expected to possess. As highlighted through the works of Wilensky (1964, p. 145), Abbott (1988), Barnett (1994) and Eraut (1994) the lay public will not recognise professional status for a domain area in which everyone is an expert. Therefore, it is accepted that corresponding with the writings of Abbott (1988), Barnett (1994), and Eraut (1994), professional knowledge is usually presented through a formal curriculum linked to codified bodies of systematic knowledge. This provides trustworthiness an academic basis for any profession accordant with the sciences, knowledge of constructed model of social organisation and practices that underpin it.

3.8 Curriculum as a vehicle to professionalism

As a vehicle to professionalism curriculum is a term with a long history, originally used by both Plato and Aristotle to describe the subjects taught during the classical period of Greek civilization (Marsh, 1986, pp. 3-9). Historically curriculum drew on a subject form approach (content), which is still used in modern times, but has expanded to include a broader range of educational topics, beyond the classical subjects such as philosophy and mathematics (p. 3). The term curriculum is now used very variedly (Peters, 1973, p. 2), where a clear distinction between concept and structure is emphasised by many authors (Kelly, 1982, pp. 6-7; Toombs & Tierney, 1993, p. 177).

Curricula are considered to have at least two aspects, where the use of the word denotes content of a particular subject, or reference to the total programme and experiences offered by an educational institution; "it can mean anything from the 'bundle' of programs an institution offers to the individual experience of a particular student or what is taught" (Toombs &Tierney, 1993, p. 177). As Hare and Portelli (1988) observed, there exist more than 120 definitions of the term. For instance, Ornstein and Hunkins (1988, p. 6) offer six variant definitions including "a plan for action, or a written document, which includes strategies for achieving desired goals of ends", or "a plan for providing sets of learning opportunities for persons to be educated", or "a set of formal education and/or training intentions", or "a plan for learning [whereby] objectives determine what learning is important", or "a field of study, comprising its own foundations and domains of knowledge, as well as its own research, theory and principles", or "in terms of subject matter or content".

Kelly's (1982, pp. 6-7) views demarcate between the explicit and also hidden aspects (implicit), where students learn as a result of the way in which educational institutions work, such as social skills. In terms of explicitness, Kelly (1982, p.6) defines curriculum as: "a content or body of knowledge to be transmitted" .

Nevertheless, Hirst (1974) presented a slightly divergent definition, also based around the same notion that a curriculum has two elements, a content to be used and methods to be employed to bring about learning, defining curriculum as "a plan of activities aimed at achieving objectives".

Accordant with the reviewed literature, for the domain of physical security this study adopted the content and its structure definition of curriculum. Furthermore, many understandings of curriculum focus towards pedagogy, defined as the art and science of helping children learn, which is distinct from adult education. Conversely, Knowles (1980) and Jinks (1999, p. 223) make a clear distinction between the processes in which children and adults learn, defining the art and science of helping adults learn as andragogy (Jinks, 1999, p. 223). Consequently, while much discussion and debate exists in the literature regarding curriculum philosophies, the focus of this study lies in the provision of higher education for future Physical Security professionals. Contextually, a major difference between school education and higher education is that adults are saliently focused towards learning those subjects or topics they see the need to learn (Knowles, 1980, p. 47). Here the writings of Carter (1985, p. 136) and Schwartz (2012, p. 58) highlight that the planning of educational programs in this frame begins with understanding the knowledge demands of the profession.

The andragogical frame of the study is therefore driven by the fact that higher education curriculum decisions are steered by the market place as opposed to any educational philosophy or theory (Schwartz, 2012, p. 58), that is, the goal or objectives of the profession. Here a more pragmatic approach or 'competency-based' approach to curriculum can be sketched, where McNeil (1990, p. 84), Marsh (2004, p. 7) and Toombs and Tierney (1993, p. 179) (Table 3.3) point to varying multiple factor attribute approaches to curriculum. This is due to the motivations of adult learners, which differ from children. Children have a more postponed application on most of their learning. In contrast, Knowles (1980, p. 53) and more recently Tovey and Lawlor (2004, p. 24) point out that adults have a more immediacy of application. Additionally, adults engage in learning generally in response to pressures from their current situation. Adults tend to enter an educational activity in a problem-centred or performance-centred frame of mind (Knowles, 1980, p. 53; Tovey & Lawlor, 2004, pp. 11-14).

Table 3.4 The attributes approach to specialised curriculum

McNeil	**Marsh**	**Toombs and Tierney**
Purpose Methods Organization Evaluation	Content Purpose Organization	Purpose Content Organization Evaluation

From an academic orientation, people see curriculum as the vehicle by which learners are introduced to the subject matter disciplines and to organised fields of study (McNeil, 1990, p. 1). Learning is described psychologically as "a process of needs-meeting and goal-striving by individual learners" by Knowles (1980, p. 56). According to Knowles (1980, p. 89) an educational need is a discrepancy between what individuals (or organisations or society) want themselves to be, and what they actually are, the distance between an aspiration and a reality.

Thus, adopting the subject form approach in terms of content and structure for physical security relates to an understanding of the content and its application (form) in diagnosing, reasoning and treating society's protective security and crime prevention problems. If it is accepted that curriculum is "a plan of action, or a written document, which includes strategies for achieving desired goals or ends. It includes a set of formal education or training intentions; in terms of subject matter or content" (Ornstein & Hunkins, 1988, p. 6) to be learned and engaged for remuneration; then a physical security professional must be underpinned by such a formal, standardised curriculum.

Formal curricula include a mixture of generic concepts and principles, and the facts, concepts and generalizations of specific subjects or groups of subjects (Davis & Dark, 2003, pp. 2-3). Here the central objective of education is towards developing integrated structures of understanding to yield work. In this view, items of knowledge in the form of theories, concepts, facts, norms, principles and so on are not detached but rather form distinct networks of relationships (Anderson & Sosniak, 1994, p. 32). This specifically relates to the scope, organisation and sequence of the knowledge content. For example, scope refers to the amount or depth to be taught based on the student's required understanding of fields of knowledge. Organisation is the sequence of topics based on their prior knowledge requirements and sequence is the ordering of content based on these three prior design drivers (Davis & Dark, 2003, pp. 2-3). For adult learners, an appropriate principle of learning is that the sequence of the curriculum must be timed so as to be in step with their developmental tasks (Knowles, 1980, pp. 52-53).

The earlier writings of Bruner (1977, pp. 31-32) conveyed that curriculum design should be based on the structure stemming from the underlying principles of the

academic discipline, for reasons of economy. Such a view was also supported by Bloom who emphasised that the organisation of learning depends on the structure of the domain being learned. Furthermore, Bloom also expressed, congruent with cognitive constructivism's premise, that transfer and generalizability of knowledge will be determined by its structure and skill that students construct in the course of their learning (Anderson & Sosniak, 1994, p. 60).

According to Bruner (1977) the correct structure of learning permits broader generalizations, makes knowledge usable in contexts other than that in which it was learned (non-specific), and facilitates memory (heuristic retrieval from LTM) allowing the learner to relate what would otherwise be unconnected facts and therefore easily forgotten. The literature highlights that curriculum connotes the substance of what is being taught and its formal structural arrangements (Toombs & Tierney, 1993, p. 177). A view emphasised in the writings of McNeil (1990, p. 73) who states, "the concept of structure in the disciplines was widely heralded as a basis for curriculum content."

Effective organizing principles exist for curriculum where the concept of design is one such principle. This includes the content or subject matter and its presentation organisation to put it to its greatest advantage, or to have it in the most interesting, shape, form or position as possible to enhance learning. But a good design never comes from chance, it is the product of trained intelligence...By design we mean the creating of relationships (Toombs & Tierney, 1993, p. 182). Bruner (1977, p. 9) considered creating the relationships of this content of salient importance for the less able student than for the gifted ones, as it is the less able students who are most easily thrown off track by poor teaching.

Marsh's (2004, p. 19) work sees the concept of design as a framework, or "curriculum framework", defined as a group of related subjects or themes which fit together according to a predetermined set of criteria to appropriately cover an area of study, in other words, a domain of interest. Thus, the salient focus is towards individual subjects and their grouping; they are guides explicitly designed and written to assist those with a stake in the education, in their curriculum decision-making through the establishment of learning areas and relationships.

According to Bloom the most common American educational objective is the acquisition of knowledge or information. As it is expressed that problem solving or thinking cannot occur in a vacuum, it must be based upon knowledge of some of the realities (cognitions) (Anderson & Sosniak, 1994, p. 16). The study's development of a body of knowledge is informed by this body of literature, which highlights that within a domain's jurisdictional boundary, the two salient aspects of curriculum include the substance of what is being taught and its formal structural arrangements and sequencing. These aspects can be embodied within four basic components including (1) purpose, (2) content, which includes discipline based theories and facts, generalisations such as principles and concepts and propositions about cases, (3) their organisation and (4) means of evaluation in relation to professional practice.

3.8.1 Curriculum typologies

Further informing the development of a body of knowledge for physical security professionals is the view that curriculum as a term has different messages; as there exist different forms or typologies across different educational institutions, at different levels (McNeil, 1990, pp. 103-104). For example, a curriculum formulated at one level or institution may not be adopted and implemented at another. Such a varied educational state characterises security education (See Section 2.4.3). For instance, the work of McNeil (1990, pp. 103-104) highlighted five variant typologies of curriculum. First is an ideal curriculum, one which expresses desired directions as seen by those with a particular value system or specialised interests. Then, there exists a formal curriculum, which is one that is adopted by an appropriate, governing body. Third, is a perceived curriculum, which is one in which individual educators perceives the curriculum to be. Fourth is an operational curriculum, which represents what actually goes on in the classroom setting. This is followed by an experiential curriculum, what the students actually derive from and think about the operational curriculum.

Such typologies consider differing functions of educational curriculum. These functions include the delivery of a general education, a supplementary function; alternatively one designed to extend higher achieving students, exploration functions, a curriculum designed to provide individual learners opportunities to develop their personal interests. Then there exists a specialized curriculum, which is a type of curriculum in which the

current standards of a trade or profession, or academic discipline prevail (McNeil, 1990). The focus for this study is towards a specialised curriculum in which students are exposed to specific content and structure and as a result are expected to emulate those who are successfully performing as skilled workers or scholars in a domain. But other aspects must also be considered such as the hidden curriculum (McNeil, 1990), where training is different from education, distinguishing between basic academic competencies such as reading, writing, reasoning, or more general graduate attributes and subject matter competencies.

This literature also highlights that once a curriculum typology has been agreed upon or selected; a fundamental issue in curriculum planning is how to come to an agreement over what is to be taught. That is, "what knowledge to be transmitted" (Marsh, 2004, p. 19) in relation to the educational objectives (Allan, 1996, p. 1)? The work of Tyler (1949, p. 37) stressed that educational objectives should be obtainable, that is, achievable, and tangible as an observable product. This product must prescribe in advance the desired behaviour to be developed in a student in terms of topics, content and concepts, as well as what the students is expected to do with this content (Tyler, 1949, pp. 46-47). As such, congruent with the principles of andragogy, Mager (1962) presented a shift from generic educational objectives to instructional objectives that linked work competencies to formal education. This approach emphasises a link between instruction and a student's achievement of pre-specified objectives. Mager's (1962, pp. 20-36) work considered that educational objectives should fulfil three criteria: they should be 1) observable, 2) performance centric, and 3) criterion based.

Mager's (1962) work emphasised that language used in educational or instructional objectives should be less open or ambiguous and more closed to represent clearly observable student actions. Mager emphasised the inclusion of words such as write; recite; to sort; to solve; to construct; and to compare. Mager (1962) also highlighted that the conditions under which performance is to take place should be unequivocally stated in the educational objectives. This view was supported by an expression of the quality or level of performance that will be considered acceptable in each discrete objective. However, the later writings of Macdonald-Ross (1973) and Eisner (1979) emphasised the integration of specific behavioural objectives in education instead of purely instructional intentions. This approach aimed to reflect an emphasis on the behavioural

aspects of what the student will be able to do after their learning experience. Such an emphasis could not be achieved under previous conceptions, again, the difference between an aspiration and reality.

Allan's (1996, p. 99) work highlighted that further more specific learning shifts occurred, exemplifying perceived deeper learning outcomes (Allan, 1996, p. 99). Such changes were congruent with the earlier work of Eisner (1979), which emphasised subject-specific outcomes, along with student and teacher outcomes. Here informing the cognitive aspects of professionalism are subject-specific outcomes that relate directly to the content to be taught and what can be done with it. For example, "on completion of the module (subject) the student will be able to apply knowledge of crime prevention to reduce a particular crime problem". Educationally this focus provided a clear statement of what the student will be able to do as a result of their learning experiences that have been planned.

Nevertheless, such a learning statement differs from an instructional and behavioural objective in that the outcome is not expressed in a single discrete element. As competent students are expected to possess both the knowledge of crime prevention and an ability to apply it to a chosen issue. In addition, personal outcomes needed to be emphasised which are argued to be transferable to a wider range of contexts. From an educational standpoint personal transferable skills are embodied within generic academic outcomes producing broader learning outcomes (Allan, 1996, p. 102). Arguably though, these views refer back to the writings of Abbott (1988, pp. 36-41) to include the diagnosis, inference and treatment principles of professional practice. Here, such an educational objective in this context may include the learning outcome statement:

To be able to identify and compare contextual access control and crime prevention options to develop a systematic treatment plan which addresses the security risk concerns within a cost versus benefits framework. And produce a professional report and relevant supporting documentation to achieve such a plan.

This combined literature highlights that the context of this study lies in the development of a systemised body of knowledge that can be drawn on to inform and articulate an ideal curriculum of a specialized typology for future Physical Security Professionals.

Such a knowledge system would include domain specific content and general professional objectives (transferable skills), which facilitate their professional work, as a perfect solution may never be found (Toombs & Tierney, 1993, p. 181). This would include academic subject matter and competencies as they relate to core content and knowledge structure and other more general attributes considered essential for competent professional practice, along with the technique of application. The work of Peters (1973, p. 3) supported such a notion emphasising the requirement for a clear educational objective, arguing without, there can be no valid curriculum. Furthermore, such an objective must be supported by methods to bring about learning (Peters, 1973, p. 3).

Referring to the work of Ausubel (1968) (Section 1.8), a method most educators embrace to facilitate initial learning is reception learning where most understandings learners acquire of new a subject area are presented rather than discovered (discovery learning). Such presented learning can be achieved through the use of heuristics that show content, structure and relationships. In reception learning the entire content to be learned is presented in its final form, as this is the most efficient means of transmitting content of an academic discipline. This educational aspect presents the views of Marsh (2004, p. 199) who points out a fundamental question for any curriculum is "what should we teach", which in principle must be that knowledge needed to professionally practice within a domain of interest when asked within the context of adult education.

3.9 Does security possess a formal body of knowledge?

A well-established premise within the reviewed literature is that an important element of a profession is their ownership of a distinctive body of knowledge within a jurisdictional boundary. This view is explicitly supported in the work of Morris, Crawford, Hodgson, Shepherd and Thomas (2006, p. 710). Smith and Brooks (2013, pp. 1-2) also expressed this very observation for the security profession. However, in the security profession dissention exists; while some security authors such as McCrie (2004, p. 17) argue that security has created a body of knowledge through industry specific research and practices over the past generation; others argue this body of knowledge is sporadic, spread over a vast array of textual publications and held implicitly by many individual experts. That is, such texts do not explicitly enunciate

consensus content, structure and relationships as an organised system of knowledge underpinned by the science and learning on which it is based at an appropriate depth or level for future professionals.

In addition, it can also be argued that such texts do not develop general academic attributes that combine with such knowledge to produce a graduate level professional. Professionals are more recognised as formally educated (Abbott, 1988) and therefore consistent with the educational literature, the existence of texts without clear educational goals and professional quality control of understanding does not constitute a formal body of knowledge, but rather presents a diverse repository of information. Furthermore, as expressed in Section 2.4, there exists a range of professional security courses with little vetting process offering what Brooks (2007, p. 2) expresses as nothing more than allied discipline education badged as security education with little constancy. As presented in Section 2.3 consistent knowledge needs to be taught to all members of a profession, where its academic basis legitimises the profession's work. In this lucidity, deferring to the work of Manunta (1999, p. 58), a vital question must be asked, "how can a particular case or situation be assessed and performance measured?" or "how can essential matters such as liability and responsibility be decided in the current state of security education ambiguity"?

In the reviewed articulation of a professional, central emphasis is placed on defining the professions' formal knowledge system (Abbott, 1988, p. 4; Morris, Crawford, Hodgson, Shepherd & Thomas, 2006, p. 710), or body of knowledge (Martin & Guerin, 2005, p. viii) since this is considered the professions' currency (Abbott, 1988, p. 4). As Barnett (1994, p. 34) acknowledged, professionals are academically qualified people, who are in charge of a formal body of knowledge, which is sold for their remuneration. Accordingly, the work of Phinney and Smith (2009, p. 2) expressed the portrayal of knowledge structures for a discipline is an approach to researching the instruction-learning paradigm for novice learners. Organizational and structural relationships among security concepts may provide an understanding for the acquisition of concepts in memory, with a subsequent improvement in the security instructional process (Phinney & Smith, 2009, p. 2). As Bruner (1977, p. 7) expounds, grasping the structure of a subject is understanding it in a way that permits many other things to be related to it meaningfully…to learn structure in short, is to learn how things are related.

To date there does not exist an explicit, singular formal body of knowledge showing content, structure and relationships for institutions of higher education for the domain of Physical Security. Nevertheless, where community acceptance of a recognised formal body of knowledge does not exist some associations have their own certification programs that test for elements of knowledge in which they deem domain practitioners should demonstrate understanding (Morris, et al, 2006, p. 713). However, professional associations are not higher education institutions, and offer certifications accordant to their standards rather than higher education qualifications based on a clear educational objective. Such an approach perhaps misses those other attributes considered essential for professional practice, especially in light of the view that the continuity of non-specific transfer learning (Section 2.2.2) is dependent upon the mastery of the structure of the subject matter (Bruner, 1977, p. 18).

ASIS is one such organisation within the security domain that offers both their Certified Protection Professional (CPP) and Physical Security Professional (PSP) certification programs. These are based on a benchmark score attained on their multiple choice questionnaire, derived from a number (seven) of prescribed texts. Yet, accordant with the principles of what a professional is, this does not holistically meet the requirements as a formally accepted academic body of knowledge. Nor does it meet the requirements of a higher education experience or qualification teaching the science which underpins the application of core knowledge (Section 2.3) (Fox, 1994; Freckelton & Selby, 2013). Thus, Morris et al., (2006, p. 711) expressed that given the vested interests in formal bodies of knowledge, research has a significant role to play in providing theoretically grounded, empirically-based evidence of the knowledge and aspects of competence for Physical Security Professionals.

3.10 The development and mapping of bodies of knowledge

The study is grounded within the notion that institutionalising expertise (Abbott, 1988, p. 323) is not a new concept. Such a notion is supported by the work of Ericsson and Charness (1994, p. 7373) who highlight that prior to codification, knowledge in natural science and calculus which were presented as the cutting edge of mathematics a few centuries ago where only experts of that time were able to master, is in contemporary times taught in high schools and colleges. Further accentuating their point Ericsson and

Charness stress that when Tchaikovsky asked two of the greatest violinists of his day to play his concerto, they refused, deeming the score unplayable. However, in contemporary times elite violinists consider the concerto part of their standard repertory. Tchaikovsky's concerto was deemed impossible until other musicians figured how to master and describe it so that students could learn it as well (1994, p. 737). Drawing on this example, Ericsson and Charness (1994, p. 738) explain that in most domains methods for instruction and efficient training have developed in parallel with the accumulation of relevant knowledge and techniques.

However, many areas of professional knowledge are yet to be codified as it is increasingly recognised that experts often cannot explain the nature of their own expertise (Eraut, 1994, p. 102). Nevertheless, drawing on older domains such as medicine as a sociological basis (Section 2.3.1), a growing number of contemporary professions have, or are pursing clearer articulation of their knowledge systems through both sponsored projects and academic explorations. For example, as a sponsored research project, Hilburn, Hirmanpour, Khajenoori, Turner and Qasem (1999) examined the software engineering body of knowledge to use in defining competencies and establishing curriculum for the United States (US) Federal Aviation Administration's technical and management staffs. They sought to organize and catalogue the knowledge structure to provide a systematic, concise and complete description of the software engineering discipline. Their purpose was to provide the systematic foundation through a single source-reference base (p. 2). Their research produced a three tiered architecture including knowledge categories, which consist of knowledge areas, that consisted of knowledge units (p. 6) providing a strata of systematic depth and breadth for their domain's knowledge and its structure.

The work of Smart and Pontifex (1993) recognised the human resources management profession's (HRM) codified body of knowledge. This profession developed from the Personnel and Industrial Welfare Officers Association formed in 1943 into the Australian Human Resources Institute in 1992. This development was based on the four criteria for an occupation to achieve professional status, in which one of these included, "the mastery of discipline and specialized body of knowledge and skills". The development of a codified knowledge base was salient for their professionalisation process. This task was undertaken through research involving practitioners in the United

States to produce a category list of competencies. As with the security profession, this research showed a diverse and multidisciplined domain (Smart & Pontifex, 1993, p. 13), which included core and support knowledge areas. Examples of core subject areas included human resource planning, industrial relations, recruitment and selection. Examples of support subject areas included accounting, economics, quantitative methods and business law (Smart & Pontifex, 1993, p. 13). Nevertheless, consistent with Section 2.4.4 of the reviewed literature, it was acknowledged within the analysis that given the multi-disciplinary nature of the human resources management (HRM) profession, is unlikely that the body of knowledge relevant to the HRM will ever be defined to the satisfaction of all parties, resulting in a desirable body of specialised knowledge.

Martin and Guerin (2005) codified the Interior Design Profession's body of knowledge. Their process included an analysis of content of published documents from interior design entities that represented the career cycle of professional interior designers. They drew on an analysis of content, identifying keywords or knowledge areas and then weighted those knowledge areas to distinguish between the domain knowledge required in depth and that, which was considered desirable, or that which they should be aware. Then knowledge was grouped by theme and mathematically weighted. Then expert panellists, including two educators, reviewed their results assessing both their methodology and conclusions. While, limitations were acknowledged, such as highlighting that the findings were a snap shot in time, based on journals, conference proceedings, trade publications, industry reports which were organised into annotated bibliographic format. Their process documented at that time the foundational knowledge areas of the body of knowledge used by interior design practitioners.

Within the non-traditional security paradigm Brooks (2007) investigated the knowledge categories of security using a multi-phase methodology. Brooks sourced, extracted and tabulated security knowledge categories and their supporting concepts. Findings presented a table of 14 security knowledge categories and 2001 supporting subordinate concepts. Knowledge categories included criminology, emergency/contingency planning, facility management, fire science, industrial security, information and computer security, investigations, physical security, principles, risk management, security law, security management, technology and threats. In the words of Brooks

(2007), "the presented security knowledge categories provide a greater insight into defining security, through supporting the development of a security body of knowledge".

Phinney and Smith (2009) explored the knowledge structures in the electronic security sub-set and its associated concepts. They sought to understand comprehension levels and perceptions of students enrolled in a security technologies program in Singapore towards basic security-related topics. They employed multidimensional scaling (MDS) to map the formal knowledge structure for selected electronic security concepts. Their research instrument consisted of a rating scale that asked students to compare the degree of similarity between concept pairs. MDS spatially represented the data based on student's perceived relationships of the subjects. Items included: magnetic cards, video motion detection, passive infrared sensors, proximity readers, microwave sensors, microphonic cable, photoelectric beam, crime prevention through environmental design, defence in depth, and closed circuit television. Results showed that knowledge clustering occurred with similar concepts located near each other in MDS. According to Phinney and Smith (2009, p. 13) these relationships in dimensional space can provide the foundation for the development of a syllabus for instruction for student learning.

A further study by Brooks (2011) investigated security expert's knowledge structure towards, developing a security body of knowledge within the domain area of security risk management. Employing an interpretative approach Brooks (2011) also applied multidimensional scaling (MDS) as a technique to develop and present a psychometric security risk management body of knowledge. Results presented a psychometric map with a central conceptual theme of threat and the clustering of psychology risk concepts to threat, and outlying of risk assessment concepts including probability of occurrence and consequences. This map was validated through interviews with security experts. Brooks' (2011) findings presented how understanding experts' knowledge structure assists towards the development of a security body of knowledge, and improved security directed education, and that MDS and experts as a combined approach is a valid research technique.

As an exploratory review Coole and Brooks (2011) presented a physical security heuristic that captured knowledge content and structure from a first pass qualitative

analysis of printed texts. Their heuristic supported that, congruous with the writings of Martin and Guerin (2005) and Morris, Crawford, Hodgson, Shepherd and Thomas (2006), physical security does have both a knowledge content and structure which can be captured and explicitly articulated, although this was limited in its research depth. Nevertheless, the study did highlight that physical security has knowledge content, subordinate content and structure requiring further research. Their results are congruent with Abbott's (1988, p. 324) view that, once jurisdictional boundaries are established, nearly all kinds of knowledge are organisable as common resources for a body of individuals.

Consistent with the reviewed literature, Richardson (1988) expressed that professional knowledge can be codified, but arguably it must be done through some formal methodology that demonstrates generalizable validity in terms of professional education. Universities aim to develop a single codified framework, based on scientific criteria of validity, on which the profession practices (Richardson, 1988, p. 384). As Phinney and Smith (2009, p. 13) explain, it can be shown that learners acquire a knowledge structure more like that of experts after formal instruction. Brooks (2012, p. 1) considered that the task of educators is therefore to assist students with acquisition of the major concepts of a discipline into memory so that they may perceive the correct relationships among concepts of the knowledge domain. The ability of educators to understand, define, map and visually represent expert knowledge is vital if teaching and learning is to me more effective (Brooks, 2012, p. 1), and arguably consistent across teaching institutions.

Schon's work reflected that the systematic knowledge base of a profession consists of four essential properties, they are 1) specialised, 2) firmly bounded, 3) scientific and 4) standardised (Schon, 1983 cited in Eraut, 1994, p. 101). In achieving such criteria the work of Eraut (1994, p. 119) identified three essential questions that need to be addressed for every profession: (1) What is our professional knowledge base? (2) What is best learned in higher education and what is best learned in professional practice and what is best learned through an integrated course involving both contexts? (3) What has to be learned before qualification, and what is best postponed until after qualification? The syllabus for higher education is based on propositional-declarative knowledge (facts) and discipline based methods of enquiry within a strictly academic frame of

reference (Eraut, 1994, p. 116). Here curriculum development entails the selection and organisation of a set of intended learning outcomes, based on clear educational goals, in terms of what is to be learned (Posner & Rudnitsky, 1982, p. 8) and their supporting content and structure.

Furthermore, the writings of Posner and Rudnitsky (1982) highlight that educational outcomes should consider broader professional goals, where learning units should be planned in context with other units based on relationships. In addition, their sequence should logically precede, and, or follow other related learning units. Accordant with the premises of cognitive constructivism (Section 1.6) such goals are expressed through cognitive or conceptual maps, (heuristics) as these help develop educational bearings. Cognitive and concept maps are concerned with relationships among ideas, based on arranging them in some reasonable pattern or structure. These ideas include concepts, theories, propositions, facts, rules, principles and generalizations. They depict relationships among ideas in both simple and more complex terms. Such maps can be hierarchical or organised in some other way, but force the expression of broader themes, which tie the specifics together. This provides clarity and coherence to what is to be taught, highlighting the ideas central to understanding a domain of interest. Furthermore, the details of such maps may change, but the foundational ideas and their relationships are stable. The mapping process is flexible, and a map for any given set of concepts can take many forms. However, they allow educationalists to make the knowledge framework explicit, revise it, and generally be more conscious of it (Posner & Rudnitsky, 1982, pp. 8-39).

Informed from the reviewed literature, the study established the requirement to explore the systematic foundation for physical security as a professional endeavour. This is argued to exist in the knowledge categories, content and units as they relate to theories, facts, principles, generalisations, concepts as core subject knowledge (Superordinate) and supporting subject areas (Subordinate) and its cultural organisational structure. This required the development of a physical security professional's taxonomic framework represented through maps (heuristics) of propositional-declarative knowledge, arranging such knowledge in terms of form or structure. The work of Krimsky and Golding (1992, pp. 9-10) highlighted that the function of such taxonomies is to offer a conceptual net or template that provides order or structure to a domain of empirical phenomena.

Taxonomies are subsets of domains; but functionally are tangible sets of content classifications organized on the basis of a single sematic relationship (Security), which also explicitly show their relationships (Spradley, 1979, p. 137). They are instrumental category structures that serve an embryonic theoretic role for suggesting lines of enquiry, dividing up a field of study, making salient distinctions, or generating hypotheses. Taxonomies are not true or false, but rather a useful tool (Krimsky and Golding, 1992, pp. 9-10) which in this study will be used to inform towards an ideal, specialised curriculum that is firmly bounded, scientifically based and which can be standardised across educational institutions for future physical security professionals in relation to their educational objectives.

3.11 Literature reflection

This study's objectives are informed by a vast and diverse breadth of interrelated and overlapping literature, as accentuated by Figures 2.1 and 3.1. This literature includes the very notion of security, the architecture of the professions, and how higher education is instrumental in underpinning through its schooling processes modern day professionals as a group phenomenon. In this review security was philosophically professed to be about our survival as a species and well-being in terms of conditions of our day-to-day existence in the face of threats to a way of life or prosperity.

Accordingly, functionally non-traditional security was viewed as the pursuit of a stable, steady state which ensures our well-being, by protecting from threats through mechanisms of control, which if efficacious, lead to a relatively predictable environment. Regardless of contextual concern, security is predominately achieved collectively, as a group rather than individually. Such cooperation may encompass the international or national, state or regional community, individual organisations or sub-groups and individuals according to government or private ownership. Therefore, informing the contemporary notion of the physical security professional was a fused philosophical nevertheless operative discussion of the term security. This established the position that security is a broad nonetheless embedded notion within any given culture and that its vast thematic or euphemistic categories reflect its cruciality in maintaining comprehensive well-being across contemporary society.

Furthermore, the reviewed professionalism literature underscores the assertion that professions relate to groups of people who undertake complex, crucial problem solving for society accordant with an abstract knowledge system. This discourse highlighted that professions are not labels individual occupational groups such as those in the security domain apply to themselves. Rather, society and the legal fraternity through formal acknowledgement define the professions. This acknowledgement is sociologically based upon both cognitive and normative criteria underpinning both historical and present-day conceptualizations of a professional; where, (1) the job of a professional group is technically based (Cognitive), and (2), a professional adheres to a set of cultural norms (Normative) towards the solving of very crucial matters. In addition, it was acknowledged that the cognitive component is based upon the understandings of some complex department of learning or science, where professionals are braced by their acquisition of cognitive dimensions of domain specific knowledge that build over time leading to predictable outcomes. Then, their individual expertise is based on applying this knowledge, forming a cultural currency.

The reviewed literature also emphasised that professions are additionally defined in terms of their jurisdictional foci, which culturally relates to the diagnosis, inference (reasoning) and treatment of specific jurisdictional abstract problems due to their focused expertise, accordant with their relevant knowledge system (body of knowledge). Thus, professional work is bounded vertically and horizontally according to cognitive and cultural strata. Domain professional knowledge relates to domain specific, theories, concepts, principles and facts (content), supported by structure and relationships with other domain knowledge. This system's basis is built on, and encompasses the science or embodying knowledge on which their domain is constructed.

This embodying knowledge forms a system reflective of that knowledge required to practice at a professional level within specific areas of foci (Figures 3.1 and 3.3, Section 3.1). This body of knowledge embodies domain specific or what is referred as core knowledge (Superordinate), further supporting knowledge (Subordinate) and enabling general academic qualities, which interactively facilitates professional practice. Professionals are academically qualified people, who are formally educated in institutions of higher education, who are schooled in formal bodies of declarative,

propositional knowledge within a domain of foci. Formal bodies of knowledge include codified knowledge along with the relevant domain's procedures accordant with the application of such knowledge as a formal knowledge system (body of knowledge). Thus, professional knowledge relates to formally codified (explicit) knowledge representing the roles and tasks of the domain, again, to diagnose, infer and treat.

Accordant with such literature, security professionals must broadly be formally educated persons who focus towards protecting against a range of societal threats manifested by malicious actors at both macro and micro levels. As such, the concept of the physical security professional was seated accordant with this broader literature. The reviewed literature lead to the contention that jurisdictionally a contemporary physical security professional can be understood as a professional within a broader taxonomic domain (Figures 3.1 & 3.3, Section 3.1), encapsulated under the cover term security. Jurisdictionally physical security professionals are persons formally trained and skilled in the means of diagnosis, inference and treatment of loss or harm (security/crime) coupled risk concerns manifested through unlawful access and crime enablers to protect people, information or property.

Physical security professionals relate to persons formally trained to apply validated techniques according to their jurisdiction's verified knowledge base of the science or reasoning on which it is founded (2.4.1), (2.4.2), (2.4.3). Such knowledge is organised through a series of hierarchical relationships semantically related to the cover term security, which accordant with the writings of Smith and Brooks (2013), and Lab (2014) may initially stem from a vast array of other domain disciplines including: engineering, physics, architecture, criminology, psychology and sociology along with other domains that can contribute materials to such a fused knowledge system.

Consistent with knowledge-based views of expertise, the cognitive perspective has been, and remains the strongest influence across learning paradigms. Such bodies of propositional knowledge are used to both inform and develop a higher education curriculum for the professions and provide a substantive base for professional practice to be reflected or benchmarked against. This includes subjects and supporting content as well as organised structure represented through symbols and heuristics as maps of domain specific declarative, propositional knowledge. Such maps or heuristics come in

many forms, and they become the domain's symbols for communicating knowledge categories, concepts and their superordinate and subordinate relations (its structure). These heuristics or maps enhance understanding for novice learners and facilitate the remembering, either by recognition or recall, of ideas, materials or phenomena, and enable new knowledge structures to be built on their foundations, systematically integrating new information with previously established knowledge. In addition, these knowledge structures become cultural norms, standardised and taught to all new candidates of the profession setting as a minimum formal entry criteria to which competency can be assessed.

Such a view is supported by the actions of many aspiring professions, who have, as part of their journey to professionalise, sought to establish their formal knowledge base (body of knowledge) within the higher education system. This is done so that dependable educational standards can be developed which provide society with the confidence to place in their trust crucial problems to be solved in an ethical and cost effective manner. Thus, without such a formal knowledge basis and its acceptance within the broader higher educational system, the security expert will remain an individual accomplishment, but as a profession will remain highly questionable and not supported by the broader public. In short, this literature highlights that the current state of security education does not meet the standards of other, better-established professional domains.

In summary, the reviewed literature leads to the contention that the security domain as a minimum requires a generalizable ideal curriculum for each of its practice areas. Such a curriculum needs to explicitly state what the various security practice areas knowledge content includes, the structural properties of this content, and the internal relations along with broader academic attributes essential for professional practice. Only then can such a broad domain begin to be tied together accordant with definitions of security science (Section 3.7), and interconnected to the broader security domain. Formal bodies of knowledge can be codified, but they must be done through a structured formal process, a possibility which, for security education has not been explored holistically in previous research. As such, the study sought to develop cognitive maps of propositional knowledge that show both local relations and a macro organised structure towards

establishing a learning objective and generalizable knowledge system as a curriculum framework for institutions of higher education in the physical security realm.

3.12 Conclusion

This chapter established the educational guidelines for pursuing the development of a first iteration formal knowledge system for physical security professionals. Section 3.1 positioned the physical security professional within the profession's literature from Chapter 2. Then, Section 3.3 established a clear jurisdictional boundary for the study. Section 3.3 discussed defining a professional accordant with their body of knowledge, where section 3.4 presented a discussion on professional status within the security domain, and the ambiguity of security education (3.6) in relation to this literature. Section 3.7 discussed the concept of a higher education curriculum for security professionals; this was reinforced in Section 3.8, which explained a formal curriculum as a vehicle for furthering the notion of security science.

The current debate of higher education's roles for security professionals was discussed in Section 3.9. This was also reinforced in Section 3.10, which discussed the development and mapping of bodies of knowledge through formal research enquiry to reveal the content and structure of emerging professional domains. This discussion presented literature supporting focused research undertakings as a means of formally codifying occupational bodies of knowledge. The study's reviewed literature was then fused together in Section 3.11 via a reflection. The reflection articulated how the reviewed literature influences the study's enquiry boundary, research objectives and questions, and its methodological approach. The chapter then concluded with Section 3.12.

Chapter 4: Research methodology

Key Words: Exploratory, Descriptive, Explanatory, Validity, Instrument, Ethics.

4.1 Introduction

This chapter presents and describes the philosophical and methodological approach drawn on to achieve the study's research outcomes. The study incorporated a methodological architecture, seated within an ethnographic enquiry, with its theoretical foundation within the constructivism paradigm (Tynjala, 1999, pp. 363-364). The research design exemplified a mixed-methods approach (Johnson & Christensen, 2004; Fraenkel, Wallen & Hyun, 2012, p. 558). This design included a literature critique in Phase One supported by expert enrichment through physical security professional's views derived from interviews (Phase Two). Phase Three then undertook a Multidimensional Statistical Scaling (MDS) analysis to provide macro description of Phase One and Phase Two's outcomes drawing on a larger participant sample. Finally, a focus group (Phase Four) was employed as a way of interpreting, from an educational perspective, Phase One, Two and Three's outcomes in order to respond to research questions relating to physical security's body of knowledge. The methodology comprised a pilot study to test the research process and a principal study adjusted from the pilot study findings.

The study's design is presented in Section 4.1, and its phases in Section 4.2. Section 4.2.1 explains Phase One, the literature critique, as a means of exploring the explicit knowledge base of physical security. Then, Section 4.2.2 explains Phase Two, expert interviews to supplement the explicit knowledge base with expert's implicit knowledge that was not revealed by the reviewed literature. The chapter then presents Phase Three of the study (4.2.3) as a means of discovering how macro properties of physical security's body of knowledge are organised. The results from Phases One, Two and Three are educationally interpreted in Phase Four (4.2.4) where the qualitative and MDS solutions are considered by security experts towards establishing a desired curriculum framework based on a sample consensus body of knowledge. Furthermore, the chapter presents the reliability of the various phases, an explanation of the research instruments utilised (4.3) as well as limitations of the study accordant with the chosen research

methodology (4.4). Research ethical concerns (4.5) within the study are discussed followed by the chapter conclusion (4.6).

4.2 Study methodological philosophy and design

The study's methodological approach and design was guided by the combined works of: Spradley (1979), Eden (1988), Bruner (1977), Balnaves and Caputi (2001), Marsh (2004) along with Bernard and Ryan (2010). From an educational standpoint Marsh's (2004, p. 199) (Section 2.5.2) work highlighted that a fundamental question for any curriculum is 'what should we teach'? Eden's (1988, p. 8) work noted that such understanding comes from the detection of repeated themes and the construal of these using a construct system of finite number (Section 1.8). Whereas Bruner (1977, p. 19) conveyed that the better minds in a particular discipline should decide what constitutes the fundamental ideas and structure to be taught.

From a research perspective, the writings of Balnaves and Caputi (2001) emphasised three salient categories of social science research including exploratory, descriptive and explanatory typologies. According to Balnaves and Caputi (2001, p. 17) exploratory designs are valuable for investigating a new area of focus, where the goal is to discover themes and patterns in that area, as they put it, "what is there" (Bernard & Ryan, 2010, p. 8). Yet descriptive research (qualitative or quantitative) seeks to provide a detailed outline of research observations (structure). Whereas explanatory research seeks to understand in detail the results obtained (Balnaves & Caputi, 2001, p. 17) in relation to the research enquiry.

Drawing on such literature, the outcomes of the study required all three research category typologies, to explore, describe and understand the obtained data in relation to the study's phase research questions and overarching research question (Table 4.1).

Table 4.1 Study research questions

Phase	**Research Questions**
Phase One	What are the explicit knowledge concept categories for physical security as represented through repeated themes printed in security texts and their structure?
Phase Two	What are the implicit knowledge categories, and instinctive structure used by security [experts] in achieving physical security risk mitigation not extracted from the literature critique?
Phase Three	What is physical security's macro knowledge content structure as measured buried by multidimensional scaling?
Phase Four	Based on the extracted knowledge system, what are the knowledge requisites and supporting learning objectives for physical security professionals?
Research Question	What is a desirable knowledge system (body of knowledge) for physical security professionals as conveyed through the published literature and accessible professionals?

The study design included mixtures of both qualitative and quantitative research paradigms (Fraenkel, Wallen & Hyun, 2012, p. 557) where sequential phase outcomes (Tashakkori & Teddle, 1998, pp. 17-18; Johnson & Christensen, 2004, p. 51) were carried forward, informing the next phase of the study (Tashakkori & Teddle, 1998, pp. 18-19). Such mixed methods designs are defined by Tashakkori and Teddle (1998, p. 19) as "studies that are products of the pragmatist paradigm and that combine the qualitative and quantitative approaches within different phases of the research process".

The study's design included a qualitative-quantitative-qualitative approach interlinking a number of discrete, interwoven, expert-centred phases where each phase had specific outcome objectives (Johnson & Christensen, 2004, p. 51) and supporting research questions (Figure 1.3). The literature and experts informed the development of two structural models which were interpreted (explained) through the use of an expert focus group. This approach was supported in the writings of Tashakkori and Teddle (1998, p. 47) who explain that qualitative-quantitative sequences are common as many quantitative survey instruments (Phase Three) are developed from an exploratory qualitative process (Phases 1 & 2). Then Phase Four was informed by the work of Shepard, Romney and Nerlove (1972, p. 3) who pointed out that representations obtained from many quantitative approaches such as survey questionnaires including multidimensional scaling (Phase Three) are not the research end in themselves. Rather, the primary purpose of results is to facilitate a better understanding of the underlying

structural relations and clusters present in the map (Shepard, Romney & Nerlove, 1972, p. 3) (Phase Four).

This approach was also supported in the writings of Abbott (1988) and Smith (2002). Abbott (1988, pp. 8-9) conveyed that professionals' knowledge involves abstract knowledge, where the work of Smith (2002, p. 21) highlighted that experts within a discipline define the abstract structural acquisition of concepts from that discipline. Merging Abbott's and Smith's works, experts were used to develop and articulate the organized knowledge structure for the cultural domain of physical security.

4.3 Study phases

4.3.1 Phase One: Literature critique

Qualitative studies are referred to as interpretative text studies (Bernard & Ryan, 2010, p. 4) and Phase One utilized such an approach to establish a qualitative benchmark, mapping physical security's explicit knowledge and structure through literature critique. This approach drew on the format of Coole and Brook's work (2011) but with a specific jurisdictional focus. The phase established detailed knowledge content (Table 6.18) and qualitative map (heuristic) (Figure 6.2) presenting thematic categorical data (nominal scale) of the relevant concepts, principles and theories within the written domain of physical security. This approach was informed by the work of Bernard and Ryan (2010, pp. 164-165) which explained that a cultural domain incorporates "an organised set of words, concepts or sentences, all of the same level of contrast, that jointly refer to a single conceptual sphere", stating:

> Apples and oranges are the same level of contrast, where apples, oranges and lemons while contrasting, are all elements of fruit, but two levels of contrast: One level group oranges and lemons (as citrus fruits), but apples are a different kind of fruit, being more closely paired with pears and plums. (Bernard and Ryan, 2010, p. 164)

This literature explained that to map the substantive knowledge structure for the cultural domain of physical security it was necessary to establish the repeated knowledge concept categories and their supporting elements or items represented within the printed domain. The printed domain literature presented the explicitly available domain

knowledge (Kumar, 1996, p. 26), as "by far the largest trove of qualitative data is the mountain of written texts that have been produced" (Bernard & Ryan, 2010, p. 14). Superordinate and subordinate concepts and domain principles were extracted through cultural domain key word analysis (Bernard & Ryan, 2010, p. 164) and then organised according to frequency (Bedard & Chi, 1992; Ericsson & Charnes, 1997; Sternberg, 1997; Zeitz, 1997; Tynjala, 1999). This approach focused on extracting nouns, verbs and synonyms and terms as they relate to physical protection and crime prevention concerns connected with physical security.

The Collins Concise Dictionary (Krebs, 1981.) defines nouns as a word or group of words that refers to a person, place or thing (p. 881). Synonyms are defined as words that mean the same or nearly the same as another word, or a word or phrase used as another name for something (p. 1321), and synonymous is being a synonym or closely associated or suggestive (p. 1321). Whereas verbs are defined as any of a large class of words that serve to indicate the occurrence or performance of an action, and the existence of a state (p. 1445). The study utilized an annotated bibliographic approach to support this extraction where, congruous with the views of Smith (2002) as well as Nalla and Morash (2002, p. 9), the essential core functions or elements of a discipline are represented in its printed texts. The annotated bibliographic approach sought to establish clear contextual textual lineage with the physical security domain and relevant extracted concepts.

Yet, the literature highlights that it is neither necessary, nor feasible, to begin information collection from scratch (Maher, & Burke, 1991, p. 13). Rather it is desirable to know what has been done and to utilize information and findings of other works as a guide. Thus the literature was initially explored to determine themes and issues that belong together, developing a rough framework of the main themes (Kumar, 1996, p. 30) and patterns (Bernard & Ryan, 2010, p. 8) towards "uncovering what's there; experiencing the phenomenon being studied" (p. 8). In uncovering such themes or concepts and patterns within the literature the study drew on Kumar's (1996, p. 31) work that accentuated the research paradox where "until you go through the literature you cannot develop a theoretical framework and until you have developed a theoretical framework, you cannot effectively review the literature". Accordingly the study drew on priori themes to establish an efficient literature critique, which come from a

researcher's own 'first cut' understanding of any phenomenon (Bernard & Ryan, 2010, p. 55). For example:

> If you are studying the night sky, it won't take long to decide that there is a unique, large body (the moon), a few small bodies that don't twinkle (planets), and millions of small bodies that do twinkle (stars). (Bernard & Ryan, 2010, p. 55)

Consistent with the writings of Kumar (1996, p. 30) the main themes pertinent to the research topic were identified by reviewing selected texts utilizing a word count analysis, where words were sorted according to frequency count from highest to lowest. Then non-security related words were removed from the analysis such as: and, the, page and the like. The count analysis was then undertaken again; removing non-security related words, with a final count analysis undertaken. The top 49 security related words were then placed into an Excel table. The procedure was repeated for each reviewed text. Then word count data was combined through the merging of synonymous terms. Where words were merged their frequency counts were summed. Then another count analysis was conducted, and sorted from highest to lowest frequency of occurrence. This presented, through repetitive words, the 49 most frequently appearing security themes as superordinate and subordinate concepts relating to physical security risk concerns. The top 49 were tabulated accordant with their numerical values producing a text matrix (Table 6.16). This technique was accordant with the writings of Guest, MacQueen and Namey (2012, p. 6) who highlight that a mathematical analysis of text through frequency count is an orthodox form of qualitative analysis.

For the Pilot Study, the Phase One literature extraction highlighted the superordinate and subordinate concepts to be carried forward into Phase Two (Table 5.4). However, in the Principal Study, the Phase One superordinate and subordinate concepts revealed by the literature extraction (Table 5. 8) were combined with concepts presented during the Pilot Study expert interview process (Table 6.17) to develop a Phase concept table (Table 6.18).

The analysis of Phase One data drew on the concept of repetitions where according to Bernard and Ryan (2010, pp. 56-57) the more a word, concept, principle or theory as a

noun, verb or phrase appears in a text the more likely it is a salient theme. This occurred through the development of a word list where key words were identified via an analysis of text's contents pages and chapters utilizing Nvivo. Then a mathematical summation of occurrences was conducted (Bernard & Ryan, 2010, p. 65) where themes were organised accordant with the repetitive values utilizing Nvivo then placed in an Excel spread sheet for further analysis to produce knowledge concept categories. Categories are the basic building blocks of qualitative data, as categories enable researches to make sense of their data. Furthermore, categories were organised into different levels of hierarchies as a folk taxonomy to produce Table 6.19. In this approach, consistent with the writings of Spradley (1979, pp. 138-139), Johnson and Christensen (2004, p. 511) and Bernard and Ryan (2010, p. 86) sets of subcategory data fell beneath a certain higher category, and that category fell beneath an even higher level category. For example, Johnson and Christensen (2004, p. 511) highlight the analysis process adopted within the study utilizing a fruit analogy:

> In the case of fruit, some possible subcategories are oranges, grapefruit, kiwi, apples and bananas. These are all subcategories because they are part of or types of the higher level category called fruit. Yet the category of fruit maybe the subcategory of a higher category called food group. Systems of categories such as this are called hierarchies because they are layered or fall into different levels.

The Nvivo analysis complied with the writings of Johnson and Christensen (2004, p. 502) who considered a meaningful unit (a segment) to be a single word, a sentence or a complete document; the key is that the segment must have a meaning that the researcher reasons should be documented. (Johnson & Christensen, 2004, p. 511)

For structural relations Johnson and Christensen (2004, p. 515) claim that the objective is to establish relationships (relations or connections) between superordinate and subordinate categories within the data sets through mutually exclusive categories, defined as those that are clearly separate (contrasting) and distinct within the taxonomy. For example, Coole and Brooks (2011) highlighted detection as a hierarchical category, with internal detection and external detection, as subordinate, contrasting categories, supported by further subcategories such as application and contrasting key words such

as free standing (Figure 4.1). As a priori these works demonstrate and support the hierarchical proximal relations between security concepts to uncover knowledge structure. Accordant with the work of Spradley (1979, pp. 137-140) a macro-to-micro approach was adopted. Presenting the larger parts first, followed by parts included in those larger parts (internal organisation).

Figure 4.1 The priori of Coole and Brooks (2011)

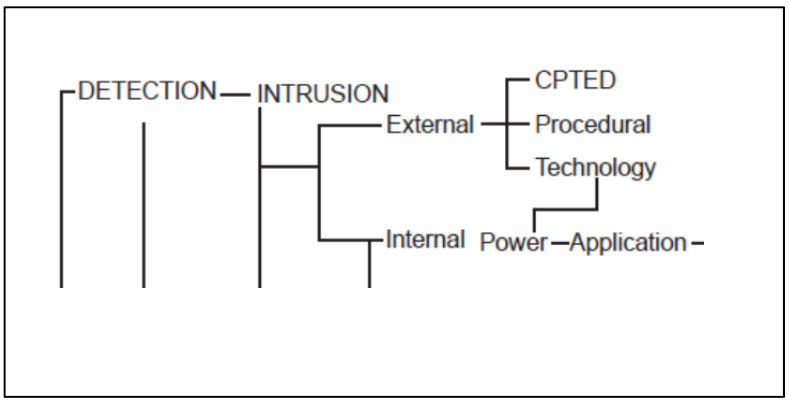


Figure 4.1 is consistent with the writings of Spradley (1979, p. 137), Johnson and Christensen (2004, p. 513) and Bernard and Ryan (2010, p. 164) showing the qualitative relations between the hierarchical category of detection and the relationships between the subordinate, contrasting categories of external and internal detection subsystems are established and explicitly highlighted.

This research method was developed from the work of Spradley (1979), and tested and supported in Coole and Brooks (2011). Therefore, the study's hierarchical analysis drew on these orderings as an already developed hierarchical system, referred to as a priori code. Priori codes are used when researchers bring an already developed coding scheme to the research project where the aim is to replicate or extend a specific line of enquiry (Johnson & Christensen, 2004, p. 508). The study utilized the assignment of categories and subcategories to analyse Phase One explicit literature data as this approach enabled the organisation of superordinate and subordinate knowledge concepts of physical security's knowledge categories through key words (codes) which became themes, into a researcher-centred cognitive map (Figure 7.4; See Section 1.8).

Therefore, for the Pilot Study, the Phase One literature extraction highlighted the superordinate and subordinate concepts to be carried forward into Phase Two (Table

5.4). These were ordered into a preliminary knowledge structure congruent with the work of Spradley (1979, p. 137) by drawing initially on the priori of Coole and Brooks (2011) to develop a Phase One hierarchical table (Table 5.5) and heuristic (Figure 5.1). For the Principal Study, the Phase One superordinate and subordinate concepts revealed by the literature extraction (Table 6. 16) were combined with concepts presented during the Pilot Study expert interview process (Table 6.17) to develop a Phase concept table (Table 6.18). Concepts were then hierarchically organised using a deductive analytical process to develop a Phase hierarchical table (Table 6.19) and heuristic (Figure 6.2). Physical security professionals were presented with the Phase concept table, hierarchical table and heuristic during Phase Two of the study.

4.3.1.1 Exploratory Phase Reliability and Validity

Supporting the reliability and validity of the literature critique and initial map is the argument emphasised by Silverman (2002, p. 229) that such textual data are in principle reliable sources for analysis. To achieve a valid result the software program Nvivo was utilized using a count analysis of occurrences, providing objective categories external from the researcher. The use of software tools for qualitative analysis is supported in the writings of Liamputtong and Ezzy (2006, p. 274) who point out that computers are both useful and more efficient in completing some tasks and can improve productivity in a research enterprise. In addition, the data extraction was supported through expert interviews (Phase Two) providing a degree of validation to Phase One outcomes.

4.3.2 Phase Two: Expert enrichment

Informed by the writings of Maher and Burke (1991, p. 13) and Cohen, Manion and Morrison (2000, p. 267), Phase Two sought to enrich Phase One outcomes through semi-structured interviews (Phase Two). The aim was to enhance the knowledge category corpus (Table 6.18) and further develop the shared (concept) heuristic (Table 6.19 & Figure 6.2) drawing on the more implicit knowledge of experts (See Section 1.8). Semi-structured interviews are common in qualitative research where a researcher draws on participants as constructors of knowledge (Liamputtong & Ezzy, 2006, p. 57). As Cohen, Manion and Morrison (2000, p. 267) explain, interviews consider that knowledge is something generated between people, often through conversation. Given

that a basic objective of research is to combine both existing and new information into contemporary knowledge outcomes (Maher & Burke, 1991, pp. 6-13), interviews provide a systematic means of discussing the domain area under investigation, thus constructing knowledge in research.

In addition, interviews are also a means to check the accuracy of, or to verify or refute the impressions a researcher makes towards their initial data (Fraenkel, 2012, p. 450) providing a degree of member checking (Creswell & Miller, 2000). Therefore, this phase also embeds a confidence level towards Phase One outcomes. Accordant with the writings of Bernard and Ryan (2010, p. 29) this method consisted of asking participants questions relating to Phase One outcomes and having them draw on their knowledge to extend on obtained results to date for further evaluation (Fraenkel, 2012, p. 451).

Therefore, Phase Two sought to extract new information (Fraenkel, 2012, p. 451) held implicitly by the experts, adding additional knowledge or practice requisites and enhanced local connections with other content areas. The interview participants for the study (security experts) stemmed from the broad fields highlighted in Table 1.2 with a concentration towards physical security (Table 5.6 & 7.2). This utilized a small sample for both the pilot study (N = 3) and the principal study (N = 9), as it is well acknowledged in the research literature that for such studies (qualitative) very few participants are required (Rundblad, 2006, p. 2). As Kopala and Suzuki (1999, p. 38) state, "qualitative research is exploratory, done with a smaller research sample focusing on a relatively unknown subject, and is often a precursor to quantitative means". The aim was to add experts' implicit knowledge to the depth of the literature critique (explicit knowledge) due to their specialised subject matter expertise and where possible add expert validation to the conceptual map (Member checking). The expert interviews elicited knowledge concept categories that were not uncovered during the literature critique phases, yet considered essential for professional practice by the experts.

Participants were contacted via telephone call or email and asked if they would participate in the study based on their professional standing or due to professional referral. The genuine purpose of the research was explained to solicited professionals. Once participants agreed, a time was arranged that was suitable for both the participants

and the researcher. Interviews were conducted either at the researcher's office, the participant's place of selection or via telephone. All participants were provided with an information sheet and informed of the study's objectives, along with an informed consent form prior to commencement of the formal interview. Once informed consent was notarised the interview commenced. All interviews were recorded utilizing a digital recorder and later transcribed verbatim for analysis through a transcription service.

The focus was on presenting extracted knowledge concept categories (Fraenkel, Wallen & Hyun, 2012, p. 453) from Phase One outcomes including Phase One knowledge concept tables, hierarchical tables and qualitative heuristics to the experts towards cueing their richly cross referenced professional knowledge of the physical security domain from their long term working memory. For the pilot study, the phase objective was therefore to draw out implicit knowledge concepts not extracted from the reviewed texts. However, for the principal study the phase objective was to present to the experts the extracted concepts from the literature along with those novel concepts extracted from the experts in the pilot study as a fused taxonomic framework and seek additional knowledge concept categories not yet uncovered.

Furthermore, due to participant feedback there were slight differences in the interview questions used between the pilot and principle studies. Notably a question regarding the merging of synonymous terms towards developing a common language priori for the principal study was removed. This approach was informed by the work of Manunta (1999) who highlighted that security lacks such common language. The issue of common language in research was noted by Jaques (1989, p. 7) which expressed that any true science must have a language of univocally defined concepts. Jaques stated, "without such clear meaning it is impossible to think, or to test propositions, or to talk to one another with any hope of understanding; and you certainly cannot train people". Nevertheless, on review of the pilot study data and participants' feedback this procedure was not continued in the principal study. Participants felt that a study of language in security was a study in and of itself, and as such, the principal study adopted the lead of Brooks (2008, p. 154) and did not attempt to provide precise concept definition, allowing the experts to define their own understanding through relationship of concepts

or knowledge structure. The final outcome of this phase was the refinement of the phase knowledge tables, hierarchical tables and knowledge heuristics.

Phase Two of the study used a qualitative, interpretative approach for interview analysis (Cohen, Manion & Morrison, 2000, p. 282) within the content and thematic analysis paradigms (Liamputtong & Ezzy, 2006, p. 260). This method incorporated both inductive and deductive approaches, sequentially guided by the physical security taxonomy of Coole and Brooks (2011). The inductive analysis was used to identify content in terms of initial concepts that emerged from the interview data transcripts. Content analysis led to the development of themes. Emerging themes supported the redevelopment of the map (priori) by drawing on experts' implicit knowledge. The term theme/s was drawn on as an expression to explain the fundamental notions a researcher is attempting to describe which are referred to in social science through different terms by different authors (Bernard & Ryan, 2010), such as categories (Glaser & Strauss, 1967), codes (Miles & Huberman, 1994), labels (Dey, 1993:96), segments (Tesch, 1990), thematic units (Krippendorff, 1980b), data bits (Dey, 1993) and chunks (Miles & Huberman, 1994).

This study followed Miles and Huberman's (1994) lead and used the term categories to represent thematic meaning. As such, themes were systematically grouped and converted into content then category codes through segmentation articulated by Johnson and Christensen (2004, p. 502) as "the inductive dividing of data into meaningful units", stating "when you segment the text data, you read the text line-by-line asking if a specific segment is present and what is it's specific meaning which may be of importance for this study"? Categories were represented in separate phase tables, one for explicit (Phase One) knowledge concepts (table 6.18) and one for implicit (Phase Two) (7.2) knowledge concepts and integrated into both a Phase (7.3) then hierarchical table (7.4) followed by a heuristic map (Figure 7.2) accordant with the representation developed by Coole and Brooks (2011).

This approach is supported within the broader research literature, where Liamputtong and Ezzy (2006, p. 259) contend that the majority of qualitative research incorporates a combination of inductive then deductive theorizing. Accordant with this literature, the inductive analysis identified physical security themes using line-by-line analysis of

content within the interview transcripts towards generating additional knowledge themes, to be integrated into the existing table (Table 6.18) and heuristic (Figure 6.2). Then the deductive analysis was drawn on to organise the participant's new knowledge categories and subordinate concepts and elements into the Phase Two's data set. Deductive theorizing occurs through building from pre-existing knowledge, an approach supported in the writings of Ausubel (1968; Novak, 1993; Fraser, 1993; Tynjala, 1999) who collectively express that knowledge changes over time as it is constructed with new information added to prior knowledge.

Integrated with Phase One outcomes, the semi-structured interview questionnaire data (Phase Two) developed a combined textual and expert group, steered knowledge table (Table 7.3). Through deductive theorizing, a hierarchical table (Table 7.4) was developed accordant with the works of Spradley (1979, p. 137), Johnson and Christensen (2004, p. 513) and Bernard and Ryan (2010, p. 164) indicating local relationships centred on mutually exclusive categories. Accordingly, a heuristic figure (Figure 7.2) of knowledge categories, concepts and subordinate concepts, theories and practice principles within the cultural domain of physical security was developed. This was achieved by making physical connections between hierarchical table (Table 7.4) contents to produce Figure (7.2) a qualitative hierarchical knowledge structure heuristic that graphically presents a snap shot of physical security's knowledge system. Nevertheless, such an analysis only shows local connections rather than macro structure, as Bernard and Ryan (2010, p. 169) point out, the whole idea of a cultural domain is that the content is shared. Phase Two was therefore enhanced through Phase Three.

The development of Phase Three was informed by the writings of Bernard and Ryan (2010, p. 169) who state "once we know content of a cultural domain, the next step is to examine how they are related to each other, which can be achieved by asking participants within the domain how similar or dissimilar content is" (p. 171). Therefore the knowledge table (Table 7.4) qualitative heuristic was used to inform Phase Three, the development of a multidimensional statistical scaling (MDS) survey questionnaire to be administered to a larger research sample where the outcome would reveal the macro structure as informed by a larger participant sample.

Interview data was recorded and transcribed verbatim supporting truthfulness in reporting (Schensul, LeCompte, Nastasi & Borgatti, 1999). Then following analysis converted into knowledge category codes, using both the priori of Coole and Brooks (2011), and then integrated into the existing map. This provided step one in establishing trustworthiness and validity in Phase Two's outcomes. From this point further reliability of Phase Two stemmed from the view that qualitative data itself is not what is questioned, but rather the inferences drawn from them (Maxwell, 1992, p. 283). As Maxwell (1992, p. 284) explains, for qualitative data that validity is not a sole product of any methodology, rather it pertains to the data accounts, or conclusions reached. Therefore, both descriptive and interpretative validity techniques were employed within Phase Two.

Descriptive validity refers to factual accuracy of participant accounts, and was achieved utilizing a narrative account of what participants said. Along with the transcripts the narrative account provided trustworthiness, where the narrative supported by the transcripts provides such qualitative validity. Descriptive validity was supported by interpretative validity, which relates to the proper denotation of what participants said. This was achieved again utilizing the narrative account, through participants' own language, relying as much as possible on participants' own words and concepts (Maxwell, 1992, p. 289). Then, where possible, categories of knowledge participants responded as important were supported through text references acknowledging such requisite, providing a degree of triangulation in the data (Creswell & Miller, 200, p. 126) as well. In addition, consistent with Phase One's reliability and validity, where possible outcomes were taken to other participants within the phase providing a degree of verification through member checking (Creswell & Miller, 2000).

4.3.3 Phase Three: MDS analysis

Phase Three was informed by the writings of Bernard and Ryan (2010, p. 111), who articulated that for social science a salient focus is towards uncovering how properties of enquiry are related. This Phase required a purposive sample of participants of an international nature to facilitate a multidimensional statistical scaling (MDS) analysis which sought to capture a psychometric map of security professionals organized knowledge structure for the cultural domain of physical security. This approach was

supported in the literature of Smith (2002, p. 21) who expressed that the substantive or subject matter of a domain are cognitive in nature. Cognitive studies seek to uncover mental representations or cognitive structures and their processes of change within a domain (Tynjala, 1999, p. 367), where internal representations of complex data may be represented in n-space (Michon, 1972, pp. 92-94). Bernard and Ryan (2010, p. 115) express such representations are achievable through the use of proximity matrices which represent domain content according to their similarity or dissimilarity (Bernard & Ryan, 2010, p. 115).

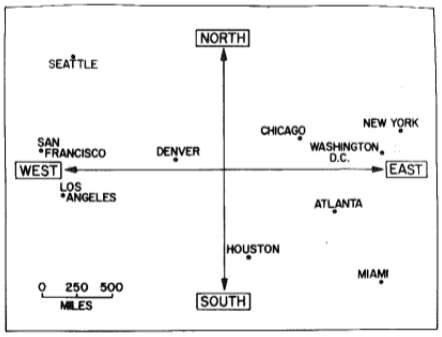
Phase Three's objective was achieved using proximity matrices questionnaires that asked participants to rate relations, or proximities, between content items, where people judge the psychological distance or closeness of survey items (Kruskal, 1978, p. 9). These ratings facilitated geographical representation of how related individual knowledge concepts and subordinate concepts were considered (Bernard & Ryan, 2010, pp. 111-115). This phase was also informed by the writings of Kruskal (1978, p. 6), who explains that the perceived similarity or dissimilarity between any two items may be expressed numerically. Thus, in similarity matrices the higher the number in each data cell, the higher the relationship (correlation) there is between these two items and the more alike they are perceived to be (Bernard & Ryan, 2010, p. 117). However, further informed by the writings of Giguere (2006), the study drew on dissimilarity data, where the further apart items are perceived to be the larger the numerical distance rating between items are and the further apart they appear in n-dimensional space.

MDS employs an algebraic equation to summarize proximity matrices' data as this equation has a geometric counterpart enabling the development of the information data picture (p. 59). Consistent with the literature this mathematical procedure represents dissimilarities of knowledge items spatially in a geographical map (Schiffman, Reynolds and Young, 1981, p. xv; p. 57). This reflects the hidden structure in the data making it easier to comprehend (Kruskal, 1978, p. 6). As Gonzalvo, Canas and Bajo (1994, p. 601) reiterate, "people's judgements of the relatedness or similarity between the members of pairs of concepts are assumed to capture the underlying organization of semantic knowledge".

In general, MDS results in a table of subjective distances between pairs of items (Michon, 1972, p. 93), arranging data into a table (data matrix) according to a shape typology. The literature indicates two MDS matrix shape typologies, a square and rectangular array (Schiffman, Reynolds and Young, 1981, p. 57). This study employed a square array as it sought to represent domain content according to their dissimilarity with every other item in the matrix, where a square matrix has the same number of rows as it does columns (p. 57) and is symmetrical (Figure 4.2) (Kruskal, 1978, p. 12). This means that every item in the matrix is related to every other item, providing a map of content structure accordant with all content.

Figure 4.2 A square MDS data matrix

CITIES	ATLA.	CHIC.	DENV.	HOUS.	L.A.	MIAMI	N.Y.	S.F.	SEAT.	WASH D.C.
ATLANTA		587	1212	701	1936	604	748	2139	2182	543
CHICAGO	587		920	940	1745	1188	713	1858	1737	597
DENVER	1212	920		879	831	1726	1631	949	1021	1494
HOUSTON	701	940	879		1374	968	1420	1645	1891	1220
LOS ANGELES	1936	1745	831	1374		2339	2451	347	959	2300
MIAMI	604	1188	1726	968	2339		1092	2594	2734	923
NEW YORK	748	713	1631	1420	2451	1092		2571	2408	205
SAN FRANCISCO	2139	1858	949	1645	347	2594	2571		678	2442
SEATTLE	2182	1737	1021	1891	959	2734	2408	678		2329
WASHINGTON D.C.	543	597	1494	1220	2300	923	205	2442	2329	



As an example, Figure 4.2 represents a square MDS data matrix and its supporting geographical map locating each US city in an n-dimensional space in which distance between pairs reflects individual city proximities of the corresponding cities (Gonzalvo, Canas & Bajo, 1994, pp. 601-602). The figure demonstrates the proximity in the first column between item 1 (Atlanta) and each of the succeeding items, the second column shows the proximities between item 2 (Chicago) and succeeding items and so on (p. 14). The square typology presents the similarity judgements of all pairs of items (Schiffman, Reynolds & Young, 1981, p. 57) where the symmetric aspects of the matrix show that the proximities in the upper half of the matrix are equal to those in the lower half (Kruskal, 1978, p. 9; Schiffman, Reynolds & Young, 1981, p.14). Thus, where variable X (New York) was highly correlated with variable Y (Washington D.C.) then these two variables were numerically closer and situated close together on the MDS plot, however the larger the value the further apart or dissimilar two items are (Breakwell, Hammond & Fife-Schaw, 2000, p. 390).

The use of MDS in the third phase of the study is supported through the writings of Michon (1972, p. 92) as well as Schiffman, Reynolds and Young (1981, pp. 3-9). These authors explain that multidimensional scaling is a viable technique suitable for investigating cognitive space representations of complex data sets based on their similarities and dissimilarities. As a research methodology MDS is suitable for revealing the underlying dimensions on which study participants base their judgements relating to knowledge structures across a domain (Zeitz, 1997, p. 52). As such, the phase objectives of MDS was to (a) represent the semantic dimensions (diagnosis & treatment) underlying the knowledge domain and (b) to arrange the concepts in the dimensional space (Gonzalvo, Canas & Bajo, 1994, pp. 601-602) presenting both dimensionality and clustering for analysis (Bernard & Ryan, 2010, p. 116).

The psychometric instrument used for the purpose of the MDS analysis was based on the results of Phase Two. Body of knowledge concepts were extracted from the Phase Two hierarchical knowledge table (Table 7.7) and heuristic map (Figure 7.4) to develop an MDS survey questionnaire instrument. However, as per the writings of Giguere (2006, p. 30) MDS questionnaires require all content items to be related to all other content items, resulting in potentially large and unworkable survey questionnaires. As such, it was necessary to reduce the number of judgements required by participants. Therefore a deductive data reduction procedure was again undertaken, where items subordinate to a clear superordinate category were removed producing Table 8.5, a list of 24 knowledge categories and subordinate content areas. Then all items were matched to each other for judgement ratings in a Qualtrics based MDS survey questionnaire.

This questionnaire was then divided into two conditions (a and b) accordant with the writings of Giguere (2006, p. 26) who acknowledged that often the number of item pairs in a design might be too high to be judged by a single participant and as such, pairs may be distributed over participants randomly assigned to different conditions of the instrument, with the set of pairs being judged by different participants completely independently. The questionnaire was then launched electronically via email, where Qualtrics as a research program managed the random assignment, data collection and initial statistical analysis, including mean and standard deviation scores. Data collection was allocated a three-month collection period, after which the survey was closed and results extracted.

The MDS survey questionnaire measured expert's ratings as ordinal level data as according to Searle (2007. p. 103) data including attitudes, opinions or ratings are to be treated as such. Therefore, while there are many MDS algorithms including ALSCAL, INDSCAL/SINDSCAL, POLYCON, MIMISSA and KRYST (Schiffman, Reynolds and Young, 1981, p. xv) this study used the ALSCAL algorithm which is suitable for both metric and non-metric scaling (Schiffman, Reynolds & Young, 1981, p. 169) and represents the best method to process ordinal data, capturing expert's perceived (Bernard & Ryan, 2010) ratings of knowledge concepts (Fraenkel, Wallen & Hyun, 2012, p. 138) for analysis.

Data categories were entered into an IBM SPSS data file in matrix format. This was done for symmetrical data (square matrix), with the upper triangle missing. Horizontal and vertical column variables represented body of knowledge category data, which were assigned coded acronyms, as SPSS does not provide for enough characters to type in full category names. These acronyms were used as category identifiers in the output graphs. Then dissimilarity data in the form of mean ratings were manually inputted into the SPSS data matrix sheet. Then, default values were entered into SPSS which included: data format as proximities-dissimilarities, data level, being ordinal, condition being Matrix, Model being Euclidean, dimension-both two and three were selected and run, Plot- common space-Transformed proximities vs. distance was selected along with all sources. Data was transformed into an MDS data map, showing macro structure.

Data analysis occurred through placing values in a half matrix configuration into an IBM SPSS program, where each item was represented by a point, where x_i indicates the point which corresponded to the i^{th} item. X is used to indicate the entire configuration of points $X_1,...,X_I$. By utilizing a coordinate system each point can be represented by coordinates. The distances between two points x_i and x_j are indicated algebraically as: $(x_i, x_j) = \text{distance from } x_i \text{ to } x_j$. This is simplified to $d_{ij} = d(x_i, x_j)$, where distances, unless indicated, refers to Euclidean distance. The central point of MDS is that distances d_{ij} between the points should correspond to the proximities δ_{ij} (pp. 15-17). This, (Figure 9) results in main diagonal of the matrix (upper left to the lower right) consist of 0's, and a symmetrical matrix. Yet as pointed out by Kruskal (1978, p. 15) MDS calculations are complex, where even the simplest versions are performed through

computer modelling. Nevertheless, provides the algorithm (1) for the ALSCAL scaling procedure.

$$\delta re = \left\{ \sum_{i} (xri - xsi)^2 \right\}^{1/2} \quad (1)$$

Through this procedure MDS revealed the data structure in the simplest terms possible (Borg & Groenen, 2005, p. 9). Both, dimensionality and underlying knowledge concept clusters were of interest for the study as the study sought to understand content, structure and relationships, along with potential sequencing as a means of informing a desirable curriculum framework. Dimensionality sought to show how the domain knowledge structure was organised at a macro level. Perceived distances (dissimilarities) revealed concept boundaries or separation towards articulating the knowledge domains as sub-category content areas of physical security and their subordinate concepts as content matter within the various sub-domains. Such an analysis is argued to be valid as MDS is a valid technique for capturing structural knowledge within a domain (Gonzalvo, Canas & Bajo, 1994, p. 602) where at the heart of MDS analysis is the dissimilarity or similarity judgements among pairs of objects as distances between points of low-dimensional multidimensional space (Borg & Groenen, 2005, p. 3) for recovering underlying structure of relationships among a group of items (Sciffman, Reynolds & Young, 1981, p. 19). The two-dimensional map showed the concepts within physical security's body of knowledge in proper relative yet separated positions to one another (Schiffman, Reynolds & Young, 1981, p. 6) as an MDS perceptual space is useful in revealing and understanding order (Schiffman, Reynolds & Young, 1981, p. 13).

A limitation of MDS is the number of dimensions researchers can conceptualise. According to Breakwell, Hammond and Fife-Shaw (2000, p. 392) three dimensions is the maximum that most people can cognitively manage. This results in an MDS analysis reducing the variables down into 2-3 or a maximum of 4 dimensions. Reducing the dimensions puts stress on the data output, affecting its reliability as it restricts the expression of variables true dimensionality due to mathematical constraints of the MDS. Stress may also be referred to as the alienation coefficient which ranges between 0 and

1 and is a goodness of fit measure considering how much the data deviates from the best possible fit. A stress measure of 0 implies perfect modelling, resulting in a perfect dimensional fit or space configuration (Kruskal, 1978, p. 25). According to this scale the smaller the coefficient the less pressure exists in the data set and therefore the better the data fit within the MDS solution. However, as Kruskal (1978, p. 25) points out, it is not truly possible to achieve a stress score of 0 for any given data set. There are several methods to measure stress for MDS and this study adopted STRESS1. To overcome the potential of a large stress measure the study drew on face validity to assess the variable set drawn from Phase Two of the study and incorporated a number of trials or iterations to reduce the measure of error in the MDS analysis (Schiffman, Reynolds and Young, 1981, p. 7).

In addition, validity was tested against the MDS source data, using Cronbach's Alpha. This measures reliability through an alpha coefficient between 0 and 1. A measure of 0 for Cronbach's Alpha means that the source data are unreliable, whereas a measure of 1 represents perfectly reliable source data (Allen & Bennett, 2012, p. 211). For the principal study Cronbach's Alpha produced a high (α=.913) value, indicating sound reliability and validity for the Phase Three survey questionnaire knowledge concept categories association with physical security.

Furthermore, as a research methodology MDS has the advantage of being low in experimenter contamination (Schiffman, Reynolds and Young, 1981, p. 3). In addition, Breakwell, Hammond and Fife-Schaw (2000, p. 390) explain another benefit of MDS as a research methodology is that the structure of the data can be examined in two salient ways. First, the regionality of the space can be examined to identify regions occupied by a particular group of variables, which for this study highlight specific sub-knowledge domains and respective separations. Second, the shape of the data plot can be examined to see if the variables arrange themselves in a straight-line or a circle. According to Gonzalvo, Canas and Bajo (1994, p. 602) and Breakwell, Hammond and Fife-Schaw (2000, p. 390), MDS captures global structural properties, an outcome recommended by Rogers (2000, p. 66) who explained the necessity to define the common threads that bind the diverseness of the domain together from the broadest possible perspective.

MDS is a valid technique to discover the underlying perceptual dimensions that people use to distinguish among items in a cultural domain (Schensul, LeCompte, Natasi & Borgatti, 1999, p. 138). Congruent with the mixed-model design (Fraenkel, et al, 2012, p. 558), Phase Three provided a description of the cultural domain knowledge concepts and subordinate concepts drawn from Phases One and Two in terms of shared knowledge including categories, content and their interrelationships as a systematized knowledge structure.

4.3.4 Phase Four: Expert focus group

Phase Four sought to understand Phase Two and Three's outcomes from an educational standpoint using a purposive sample of security experts (n=7) in a focus group paradigm. This phase compared the qualitative concept map (Figure 7.4) and MDS solution (Figure 8.2) in terms of a desired curriculum framework in relation to the epistemic aspects of the body of knowledge within a discourse analysis approach. The phase also enabled experts to add final (implicit) knowledge to the structure and articulate where their individual knowledge organisationally fit into the existing knowledge structures (cognitive maps).

Focus groups are defined by Khan and Manderson (1992, p. 57) as a qualitative methodology which aim to describe and appreciate perceptions, interpretations and beliefs of a specifically selected population to understand a particular foci from the perspective of the group participants. As Liamputtong and Ezzy (2006, p. 77) explain, such groups have shared social and cultural experiences or shared particular areas of concern.

Focus groups involve a discussion between a researcher and more than one other individual (Schensul, 1999, p. 51). Such interviews are useful for obtaining participant's interpretations of results gathered in earlier research (Schensul, LeCompte, Nastasi & Borgatti 1999, p. 52), which for this study included the earlier phase outcomes. The strength of focus groups is their capacity to produce data and insight that would be less accessible without the interaction found in a group (p. 52). The work of Liamputting and Ezzy (2006, p. 80) highlighted that such groups can be used in a variety of ways and are suitable for mixed-methods studies, enhancing the outcomes of other phases.

Phase Four acknowledged that amelioration of knowledge content could only be achieved by having experts draw on their personal understanding and shared experiences of the knowledge concepts represented within the knowledge maps due to their specialization. This was due to their extensive, implicit knowledge and experience (Zeitz, 1997, pp. 14-55) considered valuable in articulating educational requisites of core knowledge categories and their elementary subordinate subject matter for physical security professionals.

Consistent with Phase Two, participants were selected based on their professional standing, peer referral, or explicit status as published experts within the security domain. Once identified potential participants were approached via email, telephone or through industry association meetings. The focus groups were established based on a suitable day and time for participants.

At the commencement of the focus groups all participants were provided with an informed consent form for signature, where it was expressed that participation is voluntary. Once informed consent was notarised participants were reminded that the focus group would be recorded for later analysis. For the focus groups the researcher acted as the group moderator introducing, through semi-structured questionnaire, the topics of interest and facilitated the group discussion in relation to the desired phase outcomes. This phase presented the qualitative and MDS representations from Phases Two and Three, as it was premised that these structures highlighted superordinate categories and subordinate concepts of subject areas required by physical security professionals for practice within their domain and therefore should be included in a physical security curriculum.

For the pilot study, the questionnaire and supporting information was presented at the commencement of the focus group. However, as a result of feedback from the pilot study, a different approach was used for the primary study whereby participants were emailed, a week before their focus group, an explanatory sheet, along with the Phase Two's knowledge table (Table 7.6), hierarchical table (Table 7.7), qualitative heuristic (Figure 7.4) and MDS solution (Figure 8.2) and focus group interview questionnaire. This provided them with the ability to understand the questionnaire in relation to the previous phase outputs, as they were being asked to draw on these data outputs to

provide their expertise towards establishing a desirable knowledge system for future physical security professionals.

In addition, at the end of the primary study's focus group, participants were asked to write down what they saw as desirable learning objectives for a physical security curriculum on provided note pads. These were later scanned in (Appendix D) for analysis. The primary study also included an independent note taker who recorded and transcribed the proceedings (Appendix E).

The focus group interviews were recorded and transcribed verbatim into written text (Martin, 2000, p. 15) where, consistent with the writings of Schensul, LeCompte, Nastasi and Borgatti (1999), this enabled close and repeated analysis of the data. This transcribed text facilitated interpretation and highlighted positions towards the abstract body of knowledge as was represented by the qualitative and MDS maps.

Focus group data was analysed using a qualitative, interpretative approach (Cohen, Manion & Morrison, 2000, p. 282) within the content and thematic analysis paradigms (Liamputtong & Ezzy, 2006, p. 260). This method incorporated both inductive and deductive approaches. Analysis commenced with coding of participant's responses to the semi-structured interview questionnaire. Furthermore, for allocating content areas with their occupational category roles colour codes where assigned to knowledge categories relating to diagnosing (yellow), inferring or reasoning (pink), treatment (blue) or professional practice (orange) and then concepts fitted to these categories as appropriate. This combined with the written transcript, and participant's written objectives (primary study only), provided a means to interpret or bring to light knowledge requisites and their supporting learning objectives based on the organisation (structure) of physical security's knowledge systems.

Descriptive validity was achieved drawing on a narrative account of what participants said, supported by the transcripts as a measure of trustworthiness. Descriptive validity was supported by interpretative validity, reaching findings through the use of participant's own language, relying as much as possible on participant's own words and concepts (Maxwell, 1992, p. 289). Descriptive and interpretative validity combined provided confidence in the focus group analysis. In addition, reliability and validity was

embedded into the mixed-methods design as it applied methodological triangulation using different methods and/or types of data to study the same research question. In this approach the strength of one method offset potential weakness within others (Fraenkel, Wallen & Hyun, 2012, p. 559) where data was continually taken back to the experts for validity of interpretation. For instance, experts' opinions explaining the structural map of physical security's body of knowledge was drawn on to explain and validate the structural representation towards articulating a shared, desirable body of knowledge within the participant sample.

Validity was further enhanced through the use of an independent note taker whose notes (Appendix E) were used for cross referencing key themes emerging from this phase of the study. Combined these approaches sought to establish trustworthiness and validity in Phase Four's findings. Further reliability of Phase Four stemmed from Maxwell's (1992, p. 283) work, emphasizing the use of both descriptive and interpretative validity. For qualitative research Maxwell (1992, p. 284) explained that validity is not a sole product of any methodology, rather it pertains to the data accounts, or conclusions reached.

The focus groups were used in this phase of the study to clarify what the experts considered essential as an epistemic framework for graduate level physical security professionals including the articulation of broad educational objectives. In addition, where convergence did not initially occur, the group interviews enabled such dissention to be teased out through discussion towards achieving consensual support. Due to the complexity of this phase's objectives, outcomes were best achieved through a focus group analysis.

4.4 Research instruments

The study required three research instruments.

4.4.1 Instrument No. 1: Semi-structured interview questionnaire (1)

Research instrument number one, a semi-structured questionnaire for use in expert interviews (Appendix A-pilot study) (Appendix D-primary study), was developed from, and incorporated the enhanced physical security heuristic resulting from Phase One of the study. This instrument presented visually specific knowledge concepts, subordinate

concepts and structures within physical security's body of knowledge to security experts. Security experts were asked to respond with their acceptance of and/or disagreement of knowledge concepts as they were represented within the heuristic. In addition, experts were asked if they knew of sources which explicitly provide for further knowledge concepts or personally knew (implicit) knowledge which should be added to the heuristic and where their individual knowledge organisationally fitted into the existing knowledge structure (heuristic). This semi-structured interview questionnaire was aimed towards cueing individual expert's knowledge from their long term memory (LTM) and ensuring that their knowledge inputs are richly cross referenced with other knowledge concepts within the domain structure to provide the nominal scale data for Phase Three.

4.4.2 Instrument No. 2: Multidimensional scaling survey instrument

Research instrument number two (Appendix B-pilot study), (Appendix E-primary study) a multidimensional scaling survey questionnaire, was developed from the physical security knowledge concepts, principles, theories and underpinning subordinate concepts resulting from Phase Two. This approach is supported in the writings of Breakwell, Hammond and Fife-Shaw (2000, p. 393) who explain that even when undertaking exploratory research, such methods do require some theoretical expectations of what they might find. That is, the selection of variables will have to be informed by some theoretical position. This is referred to as a priori expectation, and for this it is best to have a yardstick (p. 385). Thus, Phase Three drew on the data set resulting from Phase Two as its yard stick. The MDS survey instrument listed paired physical security concepts where experts rated their perceptions of similarity or dissimilarity on a sliding scale (See Schiffman, Reynolds & Young, 1981, p. 23). Instrument validity was assessed for face validity supported by a pilot study trial run.

4.4.3 Instrument No. 3: Focus group interview questionnaire

Research instrument number three, an interview questionnaire for use with the focus groups, (Appendix C-pilot study), (Appendix F-primary study) was developed from, and incorporated the qualitative and MDS structural maps of physical security body of knowledge resulting from Phases Two and Three of the study. This instrument

presented visually specific knowledge concepts and structures within physical security's body of knowledge and their subordinate concepts to security experts. As stated by Fraenkel, Wallen and Hyun (2012, p. 558) mixed-methods research includes the cross-referencing of qualitative and quantitative methods to highlight convergence in research findings. As such, security experts were asked to respond with their acceptance of and or disagreement of knowledge concepts as they are represented within the domain maps towards supporting or refuting convergence in the data.

4.5 Limitations

All studies are subject to limitations (Breakwell, Hammond and Fife-Shaw, 2000, p. 247) and given the mixed-methods research design, a number of limitations within each phase of the study must be acknowledged.

Phase One drew on a literature critique as a means to extract explicit knowledge concepts and subordinate concepts for articulating a physical security body of knowledge. As such, the first limitation within the study is the initial review of literature. As Kumar (1996, p. 30) points out, the review of literature is a never ending task, yet studies are time limited. This limitation was managed by reviewing the literature in relation to the main themes (Kumar, 1996, p. 30) assisted using the priori of Coole and Brooks (2011). In addition, when reviewing literature sources Johnson and Christensen (2004, p. 400) raise the issue of the trustworthiness of the sources. To overcome this concern all resources were considered for their quality and concepts were extracted from peer reviewed or industry body-endorsed text books (Fraenkel, Wallen and Hyun (2012, p. 39) where according to Silverman (2002, p. 229) such textual data are in principle reliable sources, and are considered by Kumar (1996, p. 29) as a coherent body of knowledge.

Some of Phase One's limitations were addressed through Phase Two which took the results of the critique to experts for their assessment regarding inclusion of key themes or core concepts they considered important to the body of knowledge. Nevertheless, this approach was not without its limitations either; that is, interviews rely on participants providing accurate and complete answers to questions (Breakwell, Hammond and Fife-Shaw, 2000, p. 247). For example, the way subjects view a study can have a negative impact on their responses and the instrument used to collect their responses may suffer

from construct validity concerns (Fraenkel, Wallen and Hyun, 2012, p. 179) or demand characteristics and then provide responses according to the perceived demands of the experimenter (Martin, 2000, pp. 75-77). Alternatively participants may lie, distrust the researcher, or wish to sabotage the study (Breakwell, Hammond & Fife-Shaw, 2000, p. 247).

Such concerns need to be considered, however, the sampling selection was focused towards overcoming these concerns through individuals who were peer nominated as physical security experts (N=9) based on their extensive knowledge or ability, their experience, occupation and/or education and training such that they would not be swayed by experimenter characteristics. In addition, the questionnaire was organised in a manner that enabled observation of internal consistency across responses. This approach was also repeated for Phase Four of the study. Social science research limitations where similarity judgements can be affected by participant attitudes towards the study were also a possibility in Phase Three (Fraenkel, Wallen & Hyun, 2012). Such manifestations include the exaggeration or attenuation of similarities producing varying variances across subjects confounding the analysis. Again, this was overcome through the use of a participant sample in the form of a focus group, which was able to consider the accuracy of Phase Three outcomes according to their education and experiences.

4.6 Research ethics

In moving into the data collection phase of the study, it must be acknowledged that ethics are an essential aspect of scientific research. Fraenkel, Wallen and Hyun (2012, p. 565) highlight three salient concerns when conducting research with human participants which include the requirement to protect participant's identities, to treat all participants with respect, and protect all participants from physical and psychological harm. However, the research design did not place any participants in a state of undue discomfort physically or psychologically. However in pursuit of an ethically robust study, formal approval for conducting the study was gained from Curtin University's Ethics Committee. All participants solicited to participate in the study were given an information sheet explaining the study and its methodology.

The study's information sheet formed part of the questionnaires and highlighted that participation was voluntary and that there was no penalty for refusing to participate. There was no undue pressure placed on solicited experts who declined to participate and all participants were asked to sign an informed consent form either in writing or electronically. In addition, interviews were conducted without any time limits, and no financial or other material benefits were offered to individuals for their participation in this study.

Furthermore, for some participants there was a legal obligation, or an expressed desire to protect their identity and keep their data/personal information confidential. To ensure the confidentiality of participant's data and identities, participants were not asked to supply their last names or other identifying details outside of research data requirements (aside from signing an informed consent notification). All personal data was stored in a secure container (Filing cabinet) within a secure building. This approach ensured compliance with the principles of informed consent (Forshaw, 2004, pp. 45-48).

4.7 Conclusion

This chapter presented the philosophical and methodological approach (3.1) and supporting literature drawn on to achieve the study outcomes. The study presented a research philosophy embedded within its theoretical foundation of constructivism where knowledge created in one study phase was carried forward to inform the next phase of the study. Phase One, which included a literature critique was supported by expert interviews (Phase Two) as a further exploratory means of developing a qualitative structural map of physical security's body of knowledge. Phase Two provided the means to develop Phase Three, a multidimensional statistical scaling (MDS) questionnaire for completion by a larger sample of security professionals. This approach provided a graphical representation of the knowledge categories and subordinate categories as an organised global picture, highlighting content structure.

Finally, focus groups were employed as a way of interpreting Phase Two and Three outcomes towards responding to the study's research questions. The chapter also presented the analytical approaches employed to draw out results to be carried forward from Phase to Phase within the study. This included a discussion on the various research instruments developed and utilized to achieve individual Phase outcomes. Finally,

research ethics were discussed and study limitations were acknowledged within the chapter to ensure that the study considered both concerns of ethics when engaging with human participants and its own methodological limitations.

Chapter 5: Pilot study

5.1 Introduction

This chapter presents the pilot study, defined by Martin (2000, p. 13) as a small-scale version of a planned study. The aim is to test the proposed methodology and procedures, and make necessary changes to enhance the primary study. It also enables the researcher to develop a clear understanding of the study where "the pilot becomes the guide for the formal study". The chapter is divided into discrete sections representing different phases of the study. Section 5.2 presents Phase One of the study: a literature extraction using a word count analysis to identify salient knowledge concept categories for the field of physical security.

Section 5.3 presents Phase Two: knowledge concept category validation by expert interviews. Included in this section is participant information, interview analysis and interpretation as well as phase limitations. Section 5.4 presents Phase Three, the descriptive phase of the study undertaken via MDS survey. This section includes the MDS cluster analysis, dimensional interpretation and findings. The chapter also presents Phase Four of the study in Section 5.5 in which a focus group is used to evaluate the physical security knowledge categories and supporting learning objectives identified throughout earlier phases of the pilot study. Section 5.6 provides an interpretation of the pilot study findings, Section 5.7 includes a reflective analysis and the chapter concludes with Section 5.8.

5.2 Phase One: Annotated bibliography

There exists a growing number of security domain knowledge texts. Some are focused towards specific categories of security such as aviation security, maritime security, or water security. However, other texts are more focused towards broader concept understanding and specific practice areas within the non-traditional domain. Such texts have groundings in criminology, engineering and management sciences. For the purposes of this pilot study, the annotated bibliography focused on texts that considered the broader concepts within security with specific focus towards the physical security knowledge area. Specifically books were drawn from the ASIS requisite knowledge base as a knowledge priori.

For each text, the contents pages and chapter text (Section 3.3.1) were used to find repeated themes through key words (Kumar, 1996, p. 30) as core and supporting knowledge subject areas of physical security. These were then assigned values accordant with occurrences within the text (Section 3.3.1**)** and in each text synonymous terms were combined (Manunta, 1999; Brooks & Corkill, 2012) (Appendix G) and the count of occurrences conducted again. In addition, some frequently occurring words were dropped from the analysis. For example, international as a category word was removed, part was also removed as a category term, as was time. For each text this produced a tabulated matrix highlighting its salient physical security knowledge concept categories. Each individual text's bibliographic extractions provided the initial knowledge category inputs towards establishing a phase knowledge matrix as a shared paradigm for physical security professionals.

The bibliographic extractions uncovered the repeated themes (Eden, 1988, p.2) (Section 1.8) presenting the initial data for establishing a preliminary taxonomic structure as a knowledge system for physical security professionals. This system stemmed from the extracted knowledge categories and supporting knowledge units (subordinate knowledge), including theories, concepts, principles and facts according to the author's thesis or central claim, the repetition of key terms or ideas and the texts message and structure.

5.2.1 Phase One: Bibliographic data extraction

Text 1: Garcia, M., L. (2008). The design and evaluation of physical protection systems (2nd ed.). Boston: Butterworth-Heinemann.

The first security text reviewed in the data corpus is a textbook written by Mary Lynn Garcia from Sandia National Laboratories, Albuquerque, NM, USA. Ms. Garcia's biography explains that she is a Senior Member of the Technical Staff at Sandia National Labs. She has over 20 years' experience in science and engineering research, development, application, teaching, and project management experience of security systems and technology. Ms Garcia has been a Certified Protection Professional (CPP) since 1997. In addition, Ms. Garcia is the sole author of two significant texts within the security domain. Her first book, The Design and Evaluation of Physical Protection

Systems was initially published in 2001 and is now in its second edition (2008). Her second book, The Vulnerability Assessment of Physical Protection Systems was published in 2006. Ms Garcia's books have become embedded into many security teaching programs globally and her first book is listed as a core text for ASIS's Certified Protection Professional (CPP) program.

The Design and Evaluation of Physical Protection Systems (2nd ed.) as a text articulates that the basic principles of security are the same regardless of application and that it is their adaption to context that is of salient importance. Such a statement is supportive of the body of knowledge concept. This text strongly emphasizes a systematic approach to security through the articulation of a physical protection system (PPS). The PPS combines technical, physical and procedural elements into a barrier system to achieve contextual protection objectives. Its salient purpose is to describe how individual elements that collectively make up an effective security system achieve this through their integration (p. xvii). This text stresses security needs to have a systems approach within a problem solving paradigm, defining and understanding the protection problem accordant with risk, prior to designing the system. The text also emphasizes the importance of evaluating the design before and after implementation, along with ongoing review.

On the basis of a count analysis, using key terms representative of synonymous words where necessary (see Appendix G), Table 5.1 was developed as the knowledge concept categories for the reviewed text.

Table 5.1 Pilot study: Phase One: Text 1 thematic knowledge category data

Physical Security						
System	Threat	Security	Detection	Analysis and evaluation	Response	Delay
Facility procedures	Target identify-cation	Entry control/Access control	Alarm assessment	Risk	Communi-cations	Safety
Closed circuit television-CCTV	Barriers	Training	Intrusion detection	Interruption	Doors	Access delay
Walls	EASI Model	Lighting	View	Windows	Facility characterization	Risk assessment
Resolution	Probability of detection	Surveillance	Security principles	Fences	Communications security	Adversary sequence diagrams
Locks	Alarm communi-cation and display	Neutraliz-ation	Entry control credentials	Protection in depth	Quantitative analysis	Physical protection system design
Balanced protection	Vulner-ability assessment process	Use of force	Adversary paths	Roofs/ Ceilings	Network supervision	Legal issues

Text 2: Fischer, R. J., Halibozek, E., & Green, G. (2008). Introduction to security (8th ed.). Boston: Butterworth-Heinemann.

The second text in the data corpus is a textbook written by three authors within the security domain. Robert Fischer's biography highlights that he is a member of the Academy of Criminal Justice Sciences and holds a PhD. He is currently the President of Asset Protection Associates Inc, a security consulting company. Robert Fischer is a former Director of Illinois Law Enforcement Executive Institute and a Professor of Law Enforcement and Justice Administration at Western Illinois University. Edward Halibozek is the former Chairperson for the Aerospace Industries Association's Industrial Security Committee and is currently a member of the Board of Directors for the Chief Special Agents Association in Los Angeles in addition to being a corporate director of security for a fortune 100 Company. Gion Green is noted in the book to be a twentieth century security pioneer.

The text forms part of the ASIS international knowledge corpus and seeks to establish for the reader the basic concepts of security. In addition, the text introduces learners to the depth and breadth of the security domain in the non-traditional sense. Furthermore, the text has sought to articulate the current problems within the basic frameworks of security theory in response to the changing global posture in a post-September 11 environment. Current problems include terrorism, a new emphasis towards securing information, identity theft, transportation, contingency planning and piracy concerns. The text aims to introduce security concepts and approaches to those new to the industry as well as serving as a reference text for professional problem solving within the security domain. This text is divided into three sections; Section One presents the security domain: its history, employment options and professional development. Section Two presents the basics of defence and Section Three focuses towards specific threats and solutions within security context areas. Of significance for this study is that the text (p. 173) highlights that while every security program must be an integrated whole, and that individual elements must grow out of the needs dictated by the circumstances, the first basic line of defence is still physical security (Section 3.1).

On the basis of a count analysis, using key terms representative of synonymous words where necessary (Appendix Z), Table 5.2 was developed as the knowledge concept categories for the reviewed text.

Table 5.2 Pilot study: Phase One: Text 2 thematic knowledge category data

Physical Security						
Security	Law	Fire	The facility	Response	Terrorism	Threat
Doors	Locks	Loss prevention	Surveillance	Electric power	Reviewing reports	detection
Perimeter security	Crimes	Traffic	Fire protection	Construction	Keys	Lighting
Arrest	Security surveys	Safes and vaults	Barriers	Closed circuit television CCTV	Windows	Walls
Alarm systems	Risk analysis	Fences	Gates	Theft controls	Probability	Drugs
Delay	Inner defences	Outer defences	Criticality	Common law	Mitigation	Biometrics
Traffic controls	Technological surveillance	Seizure	Detention	Use of force	Searching	Occupational safety

Text 3: Fennelly, L. (2003). Effective physical security (3rd ed.). Elsevier. Burlington.

The third text in the data corpus is a textbook written by Larry Fennelly whose biography explains that he is a retired Director of Security for a Harvard Museum and former Harvard University Police Department Officer with more than 40 years' experience in the security domain. He attended the National Crime Prevention Institute at the University of Louisville, Kentucky and has been extensively involved with ASIS International. To date, he has written or edited 29 books collectively and is a well-known author and internationally accepted knowledge source within the security industry (crime prevention domain). Fennelly conveys that the book contains his combined knowledge and experience from his professional years. Each chapter is designed to assist a security practitioner resolve a particular and immediate dilemma and come up with practical knowledge to help solve the problem.

The book includes discrete yet interwoven themes emphasizing influences in the design of physical security including strategies within individual knowledge areas. These areas include physical barrier considerations and building fabrics, the use of technology to provide surveillance and control access as well as fire life safety. These are supported by an introduction into standards and regulations in the American context and security officers and equipment considerations. The overall theme of the text is controlling physical access to ensure that only authorized persons gain access to a facility and property.

Key theories, themes, phrases and words accentuating this author's salient thematic knowledge categories are included in Table 5.3 as a result of a word count analysis, managing synonymous terms as appropriate (see Appendix G).

Table 5.3 Pilot study: Phase One: Text 3 thematic knowledge category data

Physical Security						
Security	Locks	Doors	Risk	Surveillance	Detection	Closed-circuit television/CCTV
Fire	Lighting	Windows	Keys	CPTED	Guards	Glass
Walls	Barriers	Response	Gates	Law	Entrances	Analysis
Containers	Recording	Fences	Lock Cylinders	Lock bolts	Security surveys	Cameras
Reporting procedures	Key control	Sensors	Padlocks	Threats	Manipulation	Hinges
Picking	Entry /Access controls	Communications	Security searches	Safes	Physical design	Natural surveillance
Identification system	Badges	Alarm systems	Transmission	Illumination	Floors	Files

5.2.2 Phase One: Findings

Phase One sought to respond to the question: *What are the explicit knowledge concept categories for physical security as represented through repeated themes printed in security texts and their structure*?

The extracted data and count analysis, combined with the merging of synonymous terms, presented the top 49 key concepts, principles and theories as words or phrases forming the salient thematic knowledge concept categories for the cultural domain of physical security. This analysis included core subject and supporting knowledge areas providing a summative benchmark across all text sources, establishing a preliminary knowledge concept category table (Table 5.4).

Table 5.4 Pilot study: Phase One: Data corpus thematic knowledge categories

Physical Security						
Security	Threat	Detection systems	System	Response	Delay	Analysis and evaluation
Fire protection	Law	Doors	Locks	Surveillance	Facility characterization	Closed circuit television (CCTV)
Entry control/access control	Risk	Lighting	Barriers	Windows	Walls	Facility procedures
Terrorism	Target identification	Fences	Loss prevention	Communications	Use of force	Alarm assessment
Electric power	Reviewing reports	Perimeter security	Security surveys	Safety	Crimes	Traffic control
Training	Intrusion detection	Interruption	Safes and vaults	CPTED	Guards	Glass
Field of view	Construction	Risk assessment	Resolution	Probability of detection	Security principles	Drugs

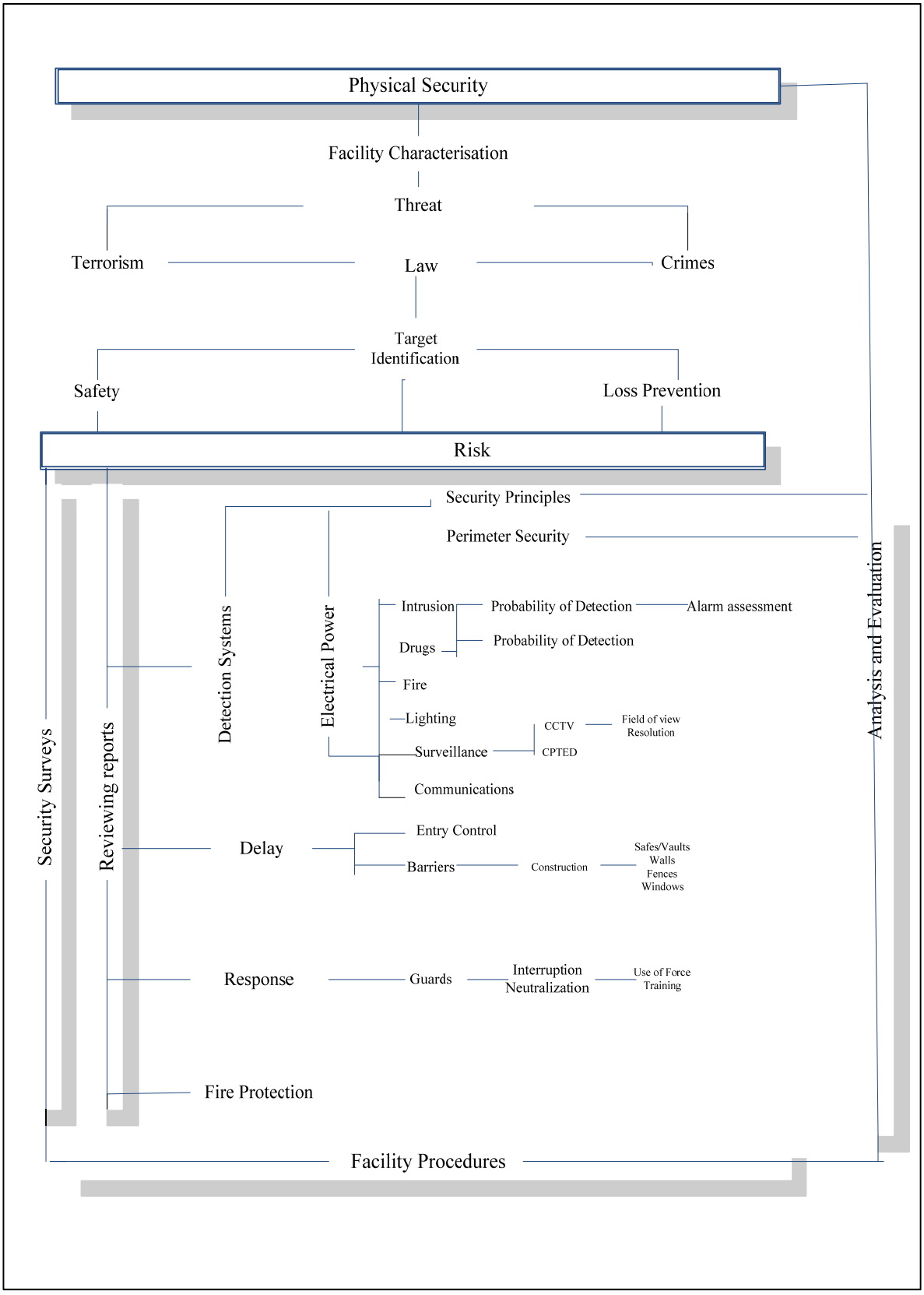
The sequential phase objective was to deductively establish a taxonomic analysis, or folk taxonomy, accordant with the writings of Spradley (1979, pp. 138-139). This taxonomy included (Table 5.5) superordinate and subordinate categorical theories, concepts and principles, along with their underpinning elements from Table 5.4. Folk taxonomies are a set of categories organized on the basis of a single semantic relationship, showing local relationships accordant with their different relational levels. The taxonomic analysis developed an initial localized cultural domain knowledge structure (Table 5.5) for physical security. This was achieved through a deductive analysis accordant with Section 4.4.3 (Figure 4.1) drawing on the precedent of Coole and Brooks (2011) as a peer reviewed code priori.

Table 5.5 led to the final Phase One outcome, which was to produce a literature-based, research-centered graphical representation – a heuristic map (Figure 5.1) -of physical security's knowledge structure. Figure 5.1, facilitated through inductive then deductive analysis, presents physical security's organized knowledge structure established through literature critique.

Table 5.5 Phase One: Hierarchical taxonomic knowledge table (adjusted from Spradley, 1979, p. 137)

<table>
<tr><td colspan="8">Security</td></tr>
<tr><td colspan="7">Facility Characterization</td><td rowspan="20">Analysis & Evaluation</td></tr>
<tr><td colspan="7">Threat</td></tr>
<tr><td colspan="3">Terrorism</td><td colspan="2">Law</td><td colspan="2">Crimes</td></tr>
<tr><td colspan="7">Target identification</td></tr>
<tr><td colspan="5">Safety</td><td colspan="2">Loss Prevention</td></tr>
<tr><td colspan="7">Risk</td></tr>
<tr><td rowspan="19">Security Surveys</td><td rowspan="19">Reviewing Reports</td><td rowspan="19">Detection Systems</td><td rowspan="19">Electric Power</td><td colspan="4">Security Principles</td></tr>
<tr><td colspan="4">Perimeter Security</td></tr>
<tr><td>Intrusion</td><td>Probability Detection</td><td>Alarm assessment</td><td></td></tr>
<tr><td>Drugs</td><td>Probability Detection</td><td></td><td></td></tr>
<tr><td>Fire</td><td></td><td></td><td></td></tr>
<tr><td rowspan="3">Lighting</td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td rowspan="3">Surveillance</td><td>CCTV</td><td>Field of View</td><td></td></tr>
<tr><td></td><td>Resolution</td><td></td></tr>
<tr><td>CPTED</td><td></td><td></td></tr>
<tr><td rowspan="3">Communications</td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td rowspan="6">Delay</td><td rowspan="3">Entry Control</td><td>CPTED</td><td></td></tr>
<tr><td>Locks</td><td></td></tr>
<tr><td>Doors</td><td></td></tr>
<tr><td rowspan="6">Barriers</td><td rowspan="6">Construction</td><td>Safes/Vaults</td></tr>
<tr><td>Walls</td></tr>
<tr><td>Fences</td></tr>
<tr><td>Glass</td></tr>
<tr><td>Windows</td></tr>
<tr><td></td></tr>
<tr><td rowspan="4">Response</td><td rowspan="4">Guards</td><td></td><td></td></tr>
<tr><td>Interruption</td><td></td></tr>
<tr><td></td><td>Use of Force</td></tr>
<tr><td>Neutralization</td><td>Training</td></tr>
<tr><td rowspan="3">Fire Protection</td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td colspan="4">Facility Procedures</td></tr>
</table>

Figure 5.1 Phase One: Preliminary physical security knowledge content heuristic



5.3 Phase Two: Expert enrichment

Accordant with Section 4.3 of the study, Phase Two aimed to elicit implicit knowledge held by security professionals which they considered essential for practice at the professional level of physical security yet not extracted through the literature critique. This phase also facilitated the merging of synonymous terms and the elucidation of more ambiguous terms. The outcome was the development of phase tables (5.6, 5.7, 5.8) and knowledge heuristic (Figure 5.2) representing superordinate and subordinate knowledge concept categories, along with their supporting content elements that make up a physical security professionals' knowledge system.

5.3.1 Participants

Phase Two sought to enhance the outcomes of Phase One by presenting the current iteration of knowledge requisites (Table 5.4, 5.5 and Figure 5.1) to participants (Table 5.6) and seeking their input to enhance these findings through a series of questions (Table 5.7) embedded into a semi-structured questionnaire (Appendix A). The objective was to draw out requisite knowledge participants believed was essential for jurisdictional practice, yet currently missing from the taxonomy.

Table 5.6 Phase Two: Expert's profiles

Name	**Profile**
Bruce	Provides protective security leadership, advice and management across numerous sectors at a senior leadership level within companies and corporations. With over 30 years' experience Bruce holds a Master of Arts (Security Management), Master of Science (MSc) Risk Management, Graduate Certificate Strategic Risk Management, and is a PhD candidate, and holds Certified Protection Professional status with ASIS International, Certified Security Consultant (International Association Professional Security Consultants), and Project Management Institute (PMI) Risk Management Professional.
Peter	Peter has over 25 years' experience providing protective security advice across a range of sectors including customs and border protection, maritime security, correctional and state infrastructure environments. Peter holds a Bachelor Degree in Security Science, and a Diploma in Project Management.
Frazer	Provides protective security leadership, advice and management across numerous sectors both as a consultant and at a senior leadership level for companies and corporations including mining operations, offshore oil and gas platforms, and government facilities both within Australia and overseas. His qualifications include a Bachelor of Science (Security, Comms and IT), Certificate of Data Communications and Certificate of Organisational Behavior and Management.

5.3.2 Administration of expert interviews

Interviews with the physical security professionals took approximately 90 minutes each, and comprised sequenced questions (Table 5.7) (Appendix A) to guide the phase outcomes. The questionnaire sought participant's thoughts relating to requisite knowledge within the domain of physical security accordant with their professional experience, along with clarification of ambiguous terms. It also sought their opinion of the knowledge structure to date, and provided them the opportunity to recommend adjustments to the hierarchical table and supporting heuristic.

Table 5.7 Phase Two: Expert interview questions

No.	**Interview questions**
1	The table shows the literature extractions top 49 thematic knowledge categories and subordinate concepts. This table was produced through the synergizing of three text's salient knowledge categories and subordinate concepts. This required a number of synonymous terms to be combined towards producing a phase table of knowledge categories and subordinate concepts. Could you please indicate your agreement/acceptance or disagreement of the following combined terms?
2	Within these knowledge categories are some physical security themes that are unambiguous in what they represent. However, there are some themes representing more ambiguous term, can you please tell me what you believe the following themes represent in terms of knowledge required for physical security professionals?
3	This table lists the salient 49 knowledge concepts and subordinate concepts for physical security's body of knowledge, do you agree with these?
4	Do you believe any of the knowledge concepts and subordinate concepts should be removed and why?
5	The top 49 knowledge categories have been organised into a hierarchical concept map to illustrate both the structure of physical security's body of knowledge including core and supporting concepts and their relations. This map aims to highlight the knowledge and structure of physical security's knowledge base towards the diagnosis, inference and treatment of security or loss coupled threat concerns manifested through unlawful access and/or crime enablers towards the protection of assets including people, information and property. Do you support this overall goal for physical security, and based on this goal do you support the structure of this map?
6	Do you believe the whole structure captures the ideas underlying physical security?
7	Do you feel that any of the knowledge concepts or subordinate concepts needs relocating and why?
8	From your knowledge of physical security, do you believe that the table and knowledge map captures the knowledge requirements for a physical security professional, and if not, what knowledge concepts and subordinate concepts are missing and why?
9	What do you feel are the three most important knowledge concepts for physical security?
10	The methodology drew on a 7 × 7 matrix to identify, categories and present core and subordinate knowledge themes and concepts resulting in the top 49. Do you believe this is sufficient or do you feel this would be best expanded to a 9 × 9 matrix to capture further subordinate knowledge concepts?
11	Do you have any further comments to enhance the tabulated knowledge categories and subordinate concepts, the heuristic map or methodology to enhance the study?

5.3.3 Interview analysis

This phase of the study sought to enhance the development and interpretation of the superordinate knowledge categories, theories and principles and their subordinate content areas representing core content units of security knowledge and supporting knowledge areas and skills for the cultural domain of physical security. As different words and terms are used to refer to the same entity in the security domain (Manunta, 1999; Brooks & Corkill, 2012) the first part of the semi-structured interview questionnaire sought participant's thoughts and feeling towards the combining of synonymous security terms to produce individual overarching (superordinate) or subordinate knowledge categories from the literature extraction. This approach reconciled the combining of synonymous terms from Phase One literature extraction, drawing on participants to partake in developing a phase table of knowledge categories and subordinate concepts.

5.3.3.1 The fusing of synonymous or similar categories

This phase sought to establish the validity of merging synonymous or similar terms. This facilitated the construction of concept categories representing the knowledge domain of physical security. Participants agreed that *threat* and *threat assessment* was both a valid and essential category for physical security professionals. As Fraser responded "it's the threat you are talking about and you look at [assess] the threat which might be assault, burglary or whatever; then you have the threat source".

In addition, participants supported the fusing of similar terms relating to *analysis and evaluation* to produce the combined category of *analysis and evaluation*. Fraser saw this as an essential component of professional practice stating:

> From a consulting point of view, analysis and evaluation is probably one of the most important parts, you look at it as a process, you have got to do it upfront, you have got to be able to firstly understand what it is you are trying to protect; if you are looking at a criticality assessment, if we are doing a risk assessment, or identify assets and criticalities, the first thing

> you classify are the critical components or items you need to protect, all that for me forms part of all the analysis and evaluation. (Frazer)

Frazer also stated, "if you put in a system, then you need to analyse and evaluate it to make sure that the system is working as it was specified to be installed, but more importantly, does it do what it is supposed to do"? Frazer made the point this is not just quantitative analysis, but also qualitative, expressing that some industries do quantitatively assess, but for others it is more about its criticality in terms of what it contributes to the system, regardless of aspects such as costs, analysis also considers the concept of contextually critical.

This view was supported by Bruce who stated that assessing the efficacy of a physical control system requires skills in analysis and evaluation in terms of technologies and also in terms of security management, as it is hard to completely separate the two. Bruce's view is congruent with Figure 3.6 (Section 3.1), where in the reviewed literature Talbot and Jakeman (2009, p. 55) highlighted that jurisdictional knowledge overlaps do exist.

Facility contextualization was another category developed through the fusing of similar terms. This category commenced as facility characterisation which was considered an essential security diagnosis component of professional practice. As Bruce pointed out:

> We are talking about the ability of practitioners or professionals to be able to fully grasp the contextual nature of what we are talking about. So to use for example, the approach to physical security within a diamond mine is a whole lot different to the approach to physical security within the university campus. And so the facility characterization is driven by the environmental requirements, but it is really important for the practitioner to grasp the real contextual boundaries. (Bruce)

Asked what was encompassed by this category Fraser responded, "you need to have an understanding of the intent, the purpose or whatever it is you are trying to achieve. Then the facility characterization is part of that, it's just a subset of the bigger picture". Furthermore, Bruce noted that "nowhere did the word context actually appear, as it has

so much influence". Bruce considered facility characterization to be part of understanding the security context, but expressed that it does not go far enough, stating, "facility characterization is driven by environmental requirements, but it is also really important for the practitioner to be able to grasp the real contextual boundaries".

Peter considered this to refer to the geographical location, but also the inputs and outputs of the organization, the physical as well as the cultural. Frazer expressed this relates to understanding what the facility does, "as depending on industry context it is going to have different requirements. If you've got a critical facility, what makes it critical"? Thus, this category was adjusted to reflect the emphasis of establishing the context, congruent with the AS/NZS ISO 31000 (2009) and Standards Australia HB 167 Security Risk Management Handbook's (2006) focus, adopting the category of *facility contextualization*. Characterization was considered an American term and for the Australian context of this study *facility contextualization* was adopted.

The adoption of an overarching category of *law* to encompass related terms was also supported by the group. As Bruce noted, "law is most often understood as legal requirements that a body or person or whatever would have to abide by, whereas legal issues may be slightly different in terms of its matter of trying to put in a process or a control. Legal issues may be difficulties of fulfilling legal requirements rather than law, which I see more as the overarching sort of legal controls". Peter supported Bruce's view stating:

> At the end of the day everything is subject to it. You have got the outside influences of Acts, there is always legislative compliance that has to be adhered to, it might not be directly security but it will be some form of legislation compliance that an organization must adhere to, usually safety is probably the most applicable one. So they are laws and probably that is the easiest way to describe it. (Peter)

Furthermore, the group supported the adoption of a broader thematic category of *movement control*. For example, Fraser expressed that movement control was a better overarching category than traffic controls, stating, "I think movement control is more encompassing, that to me would cover all the aspects associated with it as well,

particularly talking about vehicle transportation rather than any other types as well". Bruce supported the adoption of this category stating:

> It is part of our crime prevention process, control of people's movement is a control that we can institute to increase the level of protection over our assets; it is control of traffic in and out of facilities, but also within facilities. (Bruce)

The adoption of *safes and vaults* as a single category was also supported by the participants, as was the adoption of *loss prevention* as a category. Loss prevention combined *theft controls* and *loss prevention* into a single category. However, Bruce made the point that in engineering risk the term loss prevention is different to security, so jurisdictional boundary needed to be clearly understood. Both Peter and Frazer also agreed with loss prevention as broader thematic category, although Frazer pointed out this again refers to context stating, "although the underlying principle might be the same, what you do and how you apply it for change is contextual". Participants also felt some categories should be kept separate such as the terms *neutralization* and *use of force*. For instance, Peter considered use of force as a sub-category of neutralization, stating:

> Neutralization defines how you address or what end result that you are wanting to attain, you want to neutralize any threat either before, during or after the event has occurred. But use of force may not be what is utilized to neutralize the threat so you may not have a physical neutralization, you may have neutralized the threat through your defence in depth, or deterrence. (Peter)

In addition, Peter expressed the opinion that use of force is probably a misleading way of explaining what the function is, because, to another person if you're from a professional perspective trying to explain that to another person without background knowledge, "use of force will emphasize certain words in that phrase and they will emphasize force, and they will see force as guns, things like that. So it's probably not a good descriptor to use in a corporate environment". Frazer agreed with Peter's perspective stating "you can neutralize the situation without necessarily using force, but

I suppose it could be broken down and that could be a sub-set of that category itself, but that's a difficult one".

Finally, the group supported the removal of some categories which related more to the practice area of security management. For example, the category of *investigations* ranked numerically high in the word extraction, yet all participants supported the exclusion of this category within the context of the study.

5.3.3.2 Understanding ambiguous categories

While the embodiment of some categories was self-evident, others remained less defined in terms of what they encompassed for physical security professionals. For instance, clarification for the thematic category of *system* was sought from participants. Peter expressed that this relates to the more general systems theory, rather than individual systems such as electronic systems. Peter stated, "it is the physical, electronic, procedural elements that go into a security system, so a system at a particular site within an organization, it is the sum of the whole of all those parts". Bruce expressed the view that this relates to a broader thinking style, stating:

> The practitioner needs to have an understanding of how the physical security pillar fits into the remainder of a security management system and what requirements would be to satisfy the systematic approach. (Bruce)

Frazer concurred stating "it is the systematic approach to physical security…or a framework so to speak, under that framework you have different subsets, it relates to components or an approach".

In considering the reviewed literature (Section 3.1) and the participant's responses, System as a category was deemed to reflect systems thinking in the broader sense, and so the thematic category of *systems theory* was adopted. Furthermore, *terrorism* was another category that appeared often in the reviewed texts and clarification regarding its meaning was sought from the experts. Bruce expressed that many younger, less experienced security professionals had the wrong perception of terrorism, believing they see it as purely Islamic Jihadistic in nature. Bruce highlighted that terrorism includes a vast range of threat groups. Stating, "it includes the IRA, through to animal rights

activists…it is a sub-category of threat". This view was also expressed by Peter, who stated "I would rather put things into threat groups, to a threat context because most of your mitigation strategies address all threats".

According to Peter, "you can't deal with every group, you have got to put it into context; it may not even matter for some organisations". Agreeing with these views expressed by Bruce and Peter, Frazer expressed that too many people use the term terrorist as an off-the-cuff threat comment, "but is it a politically motivated or an issue motivated group as they are completely different to me"? Frazer explained that when you look at individual acts they are crimes and "for the physical security professional it is about how you treat the threat". Thus, *terrorism* was acknowledged as a sub-category of threat within this broader body of diagnosis knowledge.

This theme was also expressed for the category of *crime*. For instance, Bruce as with terrorism saw crime relating to establishing threat context, stating, "This goes back to your practitioner to be able to fully understand and grasp the context". Bruce explained that he would have this as "crime prevention" rather than crime, stating, "in terms of physical security that is what we are trying to do, prevent crimes". Peter as with Bruce, thought this should relate more to the threat context. Frazer supported Bruce's position stating, "a security professional should be more about crime prevention, being proactive rather than reactive". These views reflect the category of crime prevention in Table 3.1 from ASIS International (Section 3.1). As such, the study adopted the thematic category of *crime prevention*, to replace the category of crime.

Security principles was another ambiguous knowledge category and participants were asked what they believed this encompassed. Bruce responded that security principles refer to "the basic principles of security, which apply regardless, but are adjusted to context, such as the principle of controlling access, this is a principle, but applied very differently in different contexts". Peter stated that, "principles are like having an overarching set of protocols". Frazer took the stance that security principles could refer to the theoretical and practical side of things, "it could refer to defence in depth, situational crime prevention and CPTED theory, all those types of things".

Frazer further believed that security principles represents a subset of planning and design - a category not extracted from the literature - "where you would put certain principles and practices in place, to me the bigger picture of saying CPTED, situational crime prevention those types of things; it includes the theory behind what you are doing". Thus, the category of *security theories and principles* was adopted for the purposes of the study.

This discussion around the category of security principles led to the identification of additional knowledge categories which were included that were not reflected in the literature explicitly. These included *situational crime prevention*, *defence in depth*, and *planning and design*.

This phase also sought clarification for the knowledge category of *drugs*. Again, Bruce related this back to security's context, "it could relate to protecting drugs, say for a pharmaceutical company, or for a security manager trying to prevent the use of drugs". Conversely, Frazer saw drugs as a management concern rather than a physical security concern per se, stating, "from say a resource perspective it is part of their management system, part of their workforce management system is like employee governance requirements". Frazer was of the view that drugs form part of an organisation's threats, but more specifically towards safety in terms of fitness for work. As such, this category was adjusted to *drug detection* to reflect it is a subordinate category related to threats.

5.3.3.3 Physical security's knowledge categories and structure

The interview questionnaire also sought participants' views relating to the extracted knowledge categories and the supporting hierarchical Tables (5.4 & 5.5) and heuristic (Figure 5.1). Participants were asked if they believed any of the concept categories should be removed and why, or what they felt was missing for professional practice. Bruce responded that he agreed with the representations and believed they were reasonable as presented. Although Bruce did question the category of *safety*, asking, "why is safety here"? It was explained that safety was a category that kept coming forward in the physical security literature extraction (count analysis), in the context of preventing harm to people. The question was posed to Bruce, "where do you think on

the structure safety should be located"? Bruce responded that he thought it should be sitting on the same level as terrorism and crime as a threat, stating:

> I would have it as a third threat; just my thoughts. If you look at an organisation's approaches and philosophies and their missions and their goals and values, most of them support that their most important asset is their people…their people and safety around their people. So I see it as being right up there (indicating to Figure 5.1). Otherwise, I think this is a pretty good map…yeah that is my only comment, I think that safety needs to be further up the tree as a threat. (Bruce)

Peter responded that the knowledge categories were "pretty self-explanatory, although, it wouldn't make a lot of sense to somebody who didn't have a background knowledge". Peter was asked if he felt that any of the categories or subordinate concepts in the map (Figure 5.1) should be relocated, and he replied that:

> Where you have got your threat and it's a personal thing, I think that it should feed straight into threat groups, as they are interconnected, highlighting that in reality terrorism is a criminal act….if you have got specific threats then you will put in specific measures into place, however, for simplicity threat should feed into threat groups. (Peter)

The interviewer requested that Peter clarify where he thought that *target identification* should sit in relation to threat and in response Peter stated, "target identification is part of (subordinate to) your threat assessment process". Finally Frazer supported the representations (Tables 5.4 & 5.5; Figure 5.1), responding:

> Yes, because it breaks the different elements down of physical security. You can't rely on one thing, it's a combination or a systematic approach to achieving the outcome, it might be different elements in there, they all form part of that overall system, there are a lot of components in there that makes up the overall focus of physical security. (Frazer)

All participants supported the structure and believed it captured the systematic aspects of what physical security aims to achieve. Although Peter expressed that he believed physical security professionals needed to understand infrastructure; Peter stated:

> Infrastructure is a part that feeds into, you've got here your detection systems and then you have electrical power, and you have all these elements that go into, ultimately what they are. Those elements, all feed into your facilities infrastructure systems. So I think that without having that as an actual core body of knowledge it often gets missed. (Peter)

Peter affirmed that infrastructure is different to construction, "construction is about building so the physical building itself, infrastructure makes the building or facility function, like water or roads". Peter felt that infrastructure should be a category itself, arguing that professionals have to understand this, such as the bitumen road links into your access control. "If you don't understand infrastructure then I think this is a key flaw, quite often in security professionals, to be honest they don't understand infrastructure".

Furthermore, Peter also expressed that construction is a misleading category, expressing that security professionals can't be insular and must be able to communicate with other disciplines. Peter stated, "I don't think construction is the right word, I think it is something I will need to get back to you on". Peter did respond back that this should reflect structural strengths as a category, stating:

> As structural links security professionals knowledge to that of other relevant disciplines…these include architect, engineer and builder. You will have structural drawings, architectural drawings of buildings that define that building like walls etc. like that, doors those things so they go on the structural side of it. (Peter)

As such, the knowledge category of construction was adjusted accordant with these views to the category of *structural strengths*, and the category of *infrastructure* was added to the knowledge table as part of the phase outcomes.

This part also explored if participants believed any of the knowledge categories in Figure 5.1 should be relocated and why. However, in response to previous questions this was responded to with salient focus towards *threat* as a concept and its location as an overarching category and its subordinate group drivers. Then question eight asked participant's thoughts and feelings towards the captured knowledge requirements for a physical security professional. Initially Bruce responded that he did not see reference to statistical analysis, but then acknowledged that statistical analysis sits within the *analysis and evaluation* category. Bruce acknowledged this is subordinate to the broader category of analysis and evaluation, an all-encompassing knowledge category. Bruce was asked if he thought this to be an important part of professional practice, and responded stating:

> Yeah, I think it has got to the stage now where security professionals need to have at least basics of the ability to conduct some scientific analysis…we have moved on so far in the world now. I think that it is really important that the people that are sitting in these sorts of positions are able to hold their own against, well with their peers, and I talk about engineers, accountants, lawyers, those sort of things. And so in the physical security world where we are talking about technological systems big capital costs at times, I think security needs to have some scientific capability. (Bruce)

Peter believed that communications, both written and verbal, as well as presentation skills were missing. To be a professional the person should be able to articulate information to a broad audience including executives. Bruce also raised this point, stating:

> It is really important that the security program is able to communicate its goals, objectives etc., across the organization because without that you are not going to get buy in or support or whatever and in regards to the principles of risk management. One of the main principles of risk management is communication, communication and consultation. It hasn't come out yet, but that is one of the most important. (Bruce)

These expert's views are congruent with the writings of Gillespie (1981) who stated, "a professional that cannot verbally and publically express him/herself is in a bad way". As such, the knowledge category of *communications: written and verbal* was added to the knowledge category requirements for a physical security professional.

Peter also thought the broader category of *door furniture* should be included which is superordinate to, and includes locks and hinges which are subordinate to this knowledge category. He further emphasized that *infrastructure* was a salient thematic category and that electrical systems, closed circuit television, lighting, detection systems, fire systems etc., were elements of infrastructure and were subordinate to this broader knowledge category. Frazer considered that *response* was an important category but that different levels of response needed to be considered according to context. So again, understanding context appeared as a salient element of knowledge for physical security professionals. Thus, the knowledge category of *door furniture* was added to the knowledge table to reflect the terminology used by other professionals such as architects, to which locks and hinges etc. are subordinate.

The interview also sought what participants believed were the three most important knowledge concepts or categories for physical security? Bruce considered that *risk assessment*, *analysis and evaluation* and *communication* were the three most important areas of knowledge for physical security professionals (Core and general knowledge and skills). Peter considered understanding the facility (*facility contextualization*) was essential. He also considered understanding technological approaches to security as vital, and concluded with the category of *communications* (Core and general knowledge and skills). Frazer stated that this relates to knowledge of mitigation techniques you are going to use as part of your system for the protection of your assets or whatever (core treatment knowledge). This includes understanding how they work stating, "how can you say that you need to have microphonic fence mounted detection system if you don't understand how a microphonic detection system works"?

> Anyone could do a risk assessment, to say that, like you need guards, you need process, unless you understand how they are actually going to mitigate those threats. To me it is coming back to that having an understanding, theory of a science behind why you are doing it, why we are protecting

> things. It really comes down to having an understanding of the theory or science behind what we are trying to do and why we are trying to do it, to me is probably the most important thing. (Frazer)

Frazer's views emphasized a knowledge requirement for security professionals of the science that underpins the professional advice rendered. Frazer's stance is congruent with the writings of Freckelton and Selby (2013) (Section 2.3). Frazer considered that the academic knowledge was important, and then from there the professional development in industry was essential to develop professional thinking and practice.

Finally, participants were asked if they felt the methodology could be improved or if the knowledge categories and their supporting content areas needed to be numerically expanded. To this question all participants responded no, with Bruce stating, "what you have got here is pretty well encompassing and I fear that making it bigger is that the study starts to become onerous, too detailed and granular". Peter expressed that it was detailed enough as you did not want to lose the emphasis on the key points (areas). Frazer expressed this same view stating:

> You might just get information overload so to speak. The main thing is that you capture the main processes and all these things other things fall and hang off of that, but you don't need to capture everything, you need to capture the trigger points that everything hangs off of. (Frazer)

Such a view is congruent with Figures 1.1 (Section 1.4) and 3.3 (Section 3.1) accordant with the work of Abbot (1988, p. 8), which highlighted that the techniques themselves may in fact be delegated to other workers. Finally, question eleven asked participants if they had any further information that may enhance the tabulated knowledge categories and subordinate concepts, the heuristic map or the methodology? Bruce stated:

> I think it is a well-constructed methodology and I think it will deliver some very interesting results…it will set the foundation for some further more detailed research in particular areas that should show themselves as being those that need further attention. (Bruce)

Frazer also replied that he did not have any further comments to add, except that a difficulty for security and therefore this study is achieving a common language.

5.3.4 Phase Two: Findings

Phase Two sought to respond to the question:

What are the implicit knowledge category areas, and instinctive structure used by security [experts] in achieving physical security risk mitigation not extracted from the literature critique?

Participant's highlighted 16 additional categories (Table 5.8) as well as the renaming of some categories to be included into the physical security professional's knowledge corpus. In addition, in achieving this phase outcome, Phase Two also sought support for the merging of synonymous terms towards developing a priori for the primary study and sought knowledge category areas that participants believed based on their professional experience what was missing from the literature critique analysis.

Table 5.8 Phase Two: Participant centred knowledge concept categories

Physical Security			
Door Furniture	Defence in Depth	Situational crime Prevention	Infrastructure
Structural Strengths	Safes & Vaults	Electric Power	Delay
Surveillance	Windows	Glass	Walls
Drugs	Interruption	Field of View	Security Surveys
Movement control			

5.3.5 Phase Two: Interpretation

Findings from the pilot study indicate that implicit knowledge concept categories areas that physical security experts draw on to achieving security risk mitigation include a further 16 concept categories (Table 5.8) in addition to those extracted in Phase One (Table 5.4). Table 5.8 lists core security theories including Situational crime prevention and Defence in depth along with the very notion of surveillance as essential knowledge requisites. It also highlights that key concepts such as the control of movement are

essential in achieving a state of security. Furthermore, Table 5.8 highlight that physical security professionals require broader construction knowledge of areas such as infrastructure, structural strengths for control measures such as walls, doors and safes and vaults. They also require knowledge of openings including windows and glass, and the ability to assess their vulnerability to the threats formally through security surveys.

Phase Two results indicate that physical security's knowledge base includes a minimum of 56 knowledge categories and distinct, yet interrelated theories, concepts, principles and facts which includes those knowledge category concepts (Table 5.9) which are connected according to their relationship with the professional goal, and organized on the basis of a single semantic relationship, represented by the word security (Table 5.10 & Figure 5.1).

Table 5.9 Pilot Study: Phase Two: Physical security knowledge concept categories

Physical Security						
Security	Threat Assessment	Detection systems	Systems Theory	Response	Delay	Analysis and Evaluation
Fire protection	Law	Doors	Locks	Surveillance	Facility Contextualization	Closed circuit television (CCTV)
Entry Control	Risk	Lighting	Barriers	Windows	Walls	Facility procedures
Terrorism	Target identification	Fences	Loss prevention	Communications Technologies	Neutralization	Alarm assessment
Electric power	Reviewing reports	Perimeter security	Security surveys	Safety	Crime prevention	Movement control
Training	Intrusion detection	Interruption	Safes and vaults	CPTED	Guards	Glass
Field of view	Structural Strengths	Risk Assessment	Resolution	Probability of detection	Security Theory and Principles	Drug Detection
Use of Force	Communications: Written/ Verbal	Planning & Design	Situational Crime Prevention	Infrastructure	Door Furniture	Defence in depth

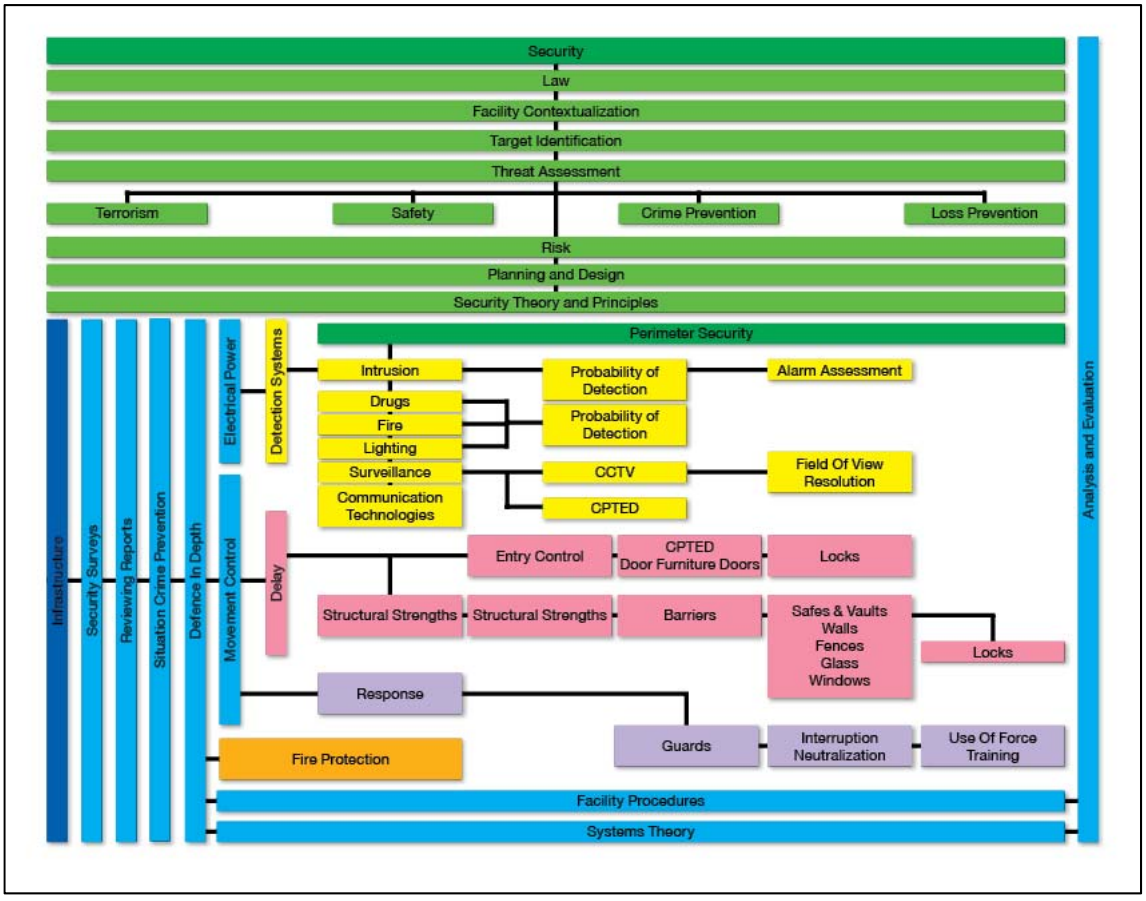
Phase Two highlighted that physical security has a system of knowledge that can be explicitly captured including core content and supporting professional knowledge (Tables 5.9 & 5.10). In addition, Phase Two also highlighted that this content has internal relations as a systemized structure that can be mapped and presented for reception learning (Figure 5.2).

Table 5.10 Phase Two: Hierarchical taxonomic knowledge table

Security													
Law													Analysis & Evaluation
Facility Contextualization													
Target Identification													
Threat Assessment													
Terrorism			Safety			Crime Prevention			Loss Prevention				
Risk													
Risk Assessment													
Planning & Design													
Security Theories & Principles													
Infrastructure	Security Surveys	Reviewing Reports	Situational Crime Prevention	Defence in Depth	Electrical Power	Detection Systems	Perimeter Security						
							Intrusion	Probability Detection	Alarm assess				
							Drugs	Probability Detection					
							Fire						
							Lighting						
							Surveillance	CCTV	Field of View				
									Resolution				
								CPTED					
							Communications: Written & Verbal						
							Technologies						
					Movement control	Delay	Structural strengths	Entry Control	CPTED				
									Door furniture	Locks			
									Doors				
								Barriers	Safes/Vaults				
									Walls				
									Fences				
									Glass				
									Windows	Locks			
						Response		Guards					
									Interruption				
										Use of Force			
									Neutralization	Training			
					Fire Protection								
					Facility Procedures								
	Systems Theory												

Table 5.10 led to the development of Figure 5.2, a physical security professional's knowledge heuristic representing core knowledge areas, their subordinate elements and their qualitative derived local structural relations. Figure 5.2 indicates that physical security's knowledge structure is hierarchically organized around the methodologies and tasks required to diagnose and prescribe protective security theories and concepts, along with their operational elements to achieve the appropriate, functional levels of control within an environmental context.

Figure 5.2 Phase Two: Physical security knowledge structure heuristic



Phase Two of the study identified core and supporting knowledge content areas that combine to achieve a predictable state through physical security (Table 5.9). This phase highlighted that when linked through hierarchical relations there exists a focused knowledge structure (Table 5.10 & Figure 5.2) that can be explicitly captured.

5.3.6 Phase Two: Limitations

This phase of the study experienced a number of methodological limitations that may have affected the findings. First the synergy of synonymous terms, as while the study attempted to address variations in language and category meanings, the interpretations and selection of language represented a snap shot of the reviewed literature and expert participant's views rather than a consensus across the broader security domain. Another limitation was the deductive analysis of category relationships rather than a statistical analysis of a larger population sample.

Phase Two highlighted some disagreement as to core and subordinate concepts, specifically with regards to Threat, and Facility Contextualization, along with subcategories of threat including terrorism and crimes. Thus Phase Three aimed to overcome these specific limitations and describe the relationships and macro structure through a larger statistically representative sample of security experts and professionals. However, it must be acknowledged that variations in language and category meaning will not be addressed in Phase Three and may be further explored in Phase Four (focus groups).

5.4 Phase Three: Macro structure analysis (MDS survey questionnaire)

Phase Three involved the administration of a survey questionnaire (Appendix B) with the results then used for an MDS analysis, a mathematical procedure for uncovering relationships between concepts. The survey was preceded by a set of instructions providing a summary overview of the study and survey completion instructions. Concepts were rated by participants (N= 14) according to their perceived dissimilarity on a ten point rating scale, where ten indicates they are highly dissimilar and therefore further apart, and one indicated they are very similar or highly related and therefore closer together. These measures were then averaged (mean) and standard deviations examined as a method for understanding shared (group) perceptions.

Not all concept categories identified in previous phases were carried forward as this would result in a survey questionnaire beyond achievable limits. Therefore, the completion of this phase required concept reduction to reduce the 56 knowledge categories and subordinate content areas to a more manageable 30 (Table 5.10). This

issue was addressed in Brooks (2008, p. 82), where it was acknowledged that such questionnaires could become too large for completion. As such, the lower order, more operational, subordinate concepts were removed for later mapping in separate studies. The aim of this phase of the study was to establish the broader content areas and their macro level structural organization rather than to map the concentrated operational connections within each category content area.

Concept reduction was achieved through a deductive analysis of superordinate and subordinate relationships. Operational level content would arguably be represented in occupational groups within the physical security knowledge strata (Figure 1.1, Section 1.4 & Figure 3.3, Section 3.1). As such, lower strata categories were removed to identify the prominent broader knowledge content for a physical security professional. For instance, Law was found to be qualitatively subordinate to Security as accordant with the writings of Beccaria (1775), Cotterell (1984) and Misiuk (2011) the law is a means of providing a state of security or the "feeling of being secure;" by regulating people's behavior. In addition, law was indicated as being superordinate to all other knowledge categories.

For obtaining functional security there emerged other strata of superordinate and subordinate concepts. Subordinate to Defence in Depth was Electrical Power as a means towards facilitating the functional electrical mechanisms of control that combine to achieve a state of security. Then, subordinate to this was the category of Detection Systems, and subordinate to this were Intrusion Detection and Drug Detection, with the subordinate primary of Probability of Detection (PD). Also subordinate to Detection Systems were Fire Detection, and Surveillance, which themselves had subordinate principles of alarm assessment, resolution and field of view. Furthermore, CPTED as a crime prevention theory was also included as subordinate to the concept of surveillance, as a major underpinning of CPTED relates to natural surveillance. Finally, Communications Technologies was also considered a subordinate content category for the broader thematic category of Detection Systems.

The thematic category of Delay was found to be subordinate to the broader concept of Movement Control, which also embodied the subordinate category of Barriers. Barriers encompassed its own subordinate content areas including Walls, Fences, Windows and

Glass. Furthermore, the thematic category of Delay also included the subordinate category of Entry Control, which included its own subordinate area of Doors and Door Furniture, which encompassed the subordinate category of Locks. The thematic category of Response, also subordinate to Defence in Depth, was shown to be superordinate to the categories of Guards, which was superordinate to Neutralization that was superordinate of Use of Force.

These strata of categories were found to be subordinate to the thematic category of Facility Procedures, which guides the response function. Finally, the thematic categories of Communications Skills: Written and Verbal, Analysis and Evaluation, and Systems Theory were considered persuasive across all professional knowledge elements for physical security professionals. Concept reduction developed Table 5.11: Superordinate knowledge concept categories for the domain of physical security.

Table 5.11 Phase Two: Superordinate knowledge categories

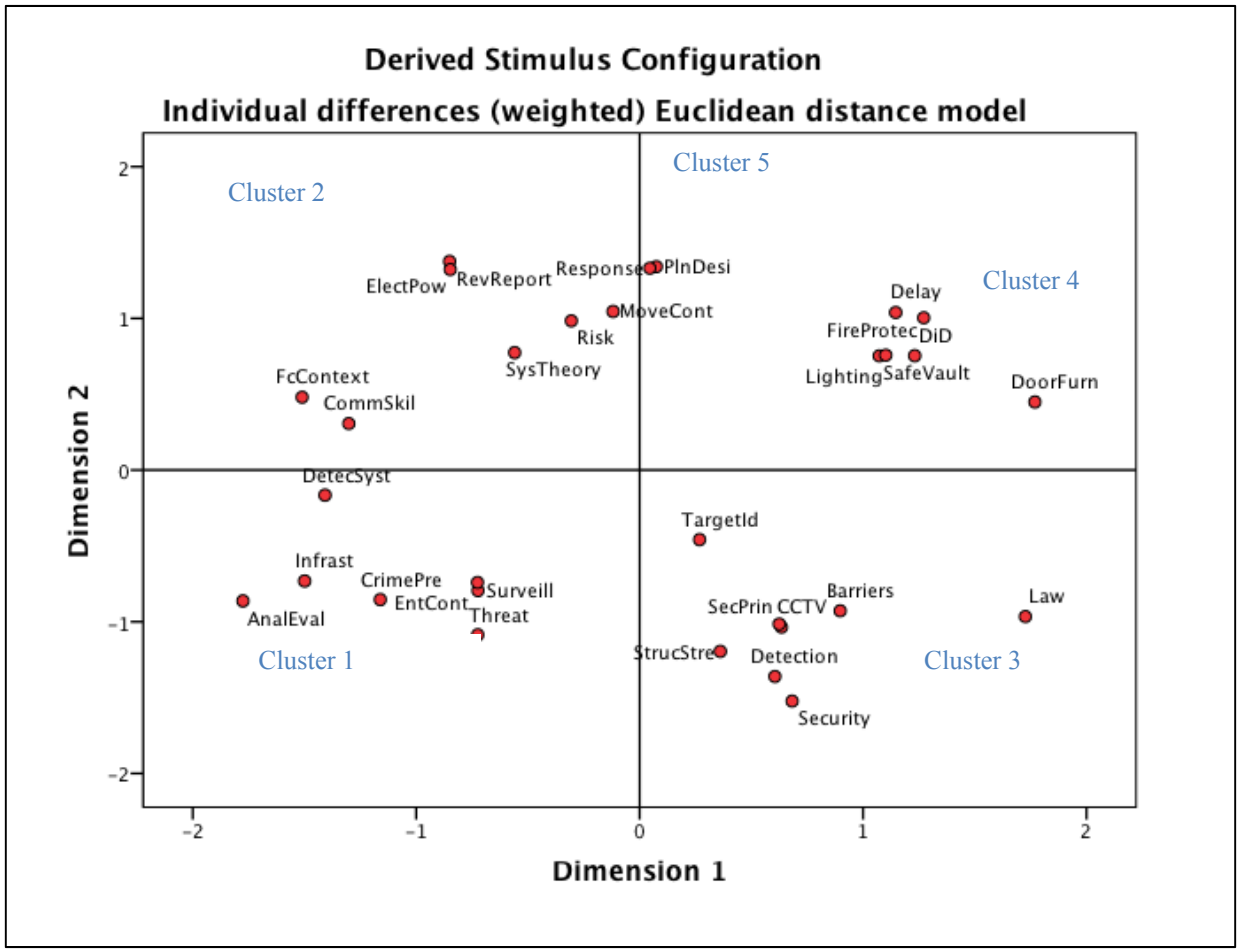
Physical Security				
Security	Law	Facility contextualization	Threat	Risk
Planning & design	Infrastructure	Analysis and evaluation	Systems theory	Security theory and principles
Defence in depth	Crime prevention	Communications Skills: Written & Verbal	Detection	Delay
Response	Structural strengths	Barriers	Lighting	Surveillance
Door Furniture	Safes and vaults	Movement control	Electric power	Entry control
Detection systems	Fire protection	Reviewing reports	CCTV	Target identification

Concept reduction knowledge categories were tested for reliability using Cronbach's Alpha. This is a test of internal consistency assessing the extent to which questions within a questionnaire tapping a single underlying construct (physical security) covary (Allen & Bennett, 2012, p. 211). Cronbach's Alpha produced a high reliability value ($\alpha = .945$) indicating a strong relationship between knowledge concept categories from Table 5.11 and physical security.

5.4.1 Phase Three: Findings

Figure 5.3 presents the SPSS output MDS spatial map capturing the global structure of the physical security domain by locating each physical security concept in an N-dimensional space accordant with proximity correlations. For Figure 5.3 the calculated distances between concept points represent participant's averaged psychological proximity of physical security's knowledge concepts.

Figure 5.3 Phase Three: MDS spatial representation of physical security concepts



The interpretation of the MDS map requires a key (Table 5.12) relating mapped concepts to those presented in Table 5.11.

Table 5.12 MDS survey key

MDS Key		
Securi = Security	Plande = Planning & design	DiD = Defence in depth
Respon = Response	Doorfu = Door furniture	Detsys = Detection systems
Law = Law	Infras = Infrastructure	Crimep = Crime prevention
Strucs = Structural strengths	Analev = analysis & evaluation	Commsk = Communications skills
Barrie = Barriers	Safeva = safes & vaults	Firepr = Fire protection
Fccont = facility contextualization	MoveCo = Movement control	RevRep = Reviewing reports
Threat = Threat	SysThe = systems theory	Detect = Detection
Light = Lighting	ElecPo = Electric power	CCTV = closed circuit television
Risk = Risk	SecPri = Security principles	Delay = Delay
Surv = Surveillance	EntCon = Entry control	TargetId = Target identification

A two-dimensional MDS map was developed consistent with the writings of Davies and Coxon (1982, p. 6), who express the need for a spatial solution of three or preferably fewer dimensions so that the structure of the entire configuration can be visually interpreted. This view is shared by Shepard (1972, p. 4) who pointed out that finding interpretable axes becomes considerably more difficult and uncertain when the number of dimensions exceeds what can be immediately apprehended in a picture or model.

The goodness-of-fit was evaluated according to Kruskal's Stress Formula 1 and the Squared Correlations. The data presented a high Stress score of 0.36351 and an RSQ of .25314 (Squared correlations in distances), which according to the MDS Stress measure, not all concepts were in their ideal spatial locality. Nevertheless, a stress score of 0.36351 was within the 0.54 stress score tolerances of Rakshit and Ananthasuresh (2008, pp. 293-294). Rakshit and Ananthasuresh demonstrated that a stress score of 0.54 was acceptable for a valid MDS analysis. By utilizing a graph of alternate dimensional settings and stress scores Rakshit and Ananthasuresh (2008, p. 293) were able to demonstrate that a stress score of 0.54 best fitted the correlational model; where both higher and lower dimensional increases in paired amino acid relations increased stress. Thus, a two dimensional map with a stress score of 0.54 was the most appropriate means of visually presenting the hidden structure in their data set.

The MDS map was interpreted using both clusters and dimensional analysis accordant with the work of Davies and Coxon (1982, p. 6) who emphasized that for interpreting

such an MDS solution, any interpretable feature of the spatial configuration, for instance clusters and dimensionality, including circular and linear orderings could be considered. Therefore MDS provided for two modes of interpretation, being clustering of concepts based on their close or distal proximity and their dimensional locality according to their cultural separation.

5.4.2 MDS Clusters

5.4.2.1 Cluster One

Clusters are identified from One to Five (Figure 5.3) with Cluster One including the concepts of crime prevention, entry control, surveillance, threat, infrastructure, analysis and evaluation, and detection systems. Central in Cluster One was crime prevention, which was closely related to entry control with a relationship mean of 1.93 and a standard deviation of 0.73, indicating that participants collectively perceive these two concepts as similar. In addition, crime prevention and threat were also considered highly related with a mean of 2.07 and a standard deviation of 1.79, indicating a reasonable degree of consensus across the sample for this pairing. Crime prevention and surveillance were also considered closely related, with a mean of 2.14 and a standard deviation of 0.66, indicating consensus for this pairing.

Crime prevention was considered related to, but slightly dissimilar from Analysis and evaluation, with a mean of 3.07. However, consensus diverged for this pairing with a standard deviation of 2.53, indicating varied perceptions of their relatedness. Crime prevention and infrastructure were also related in proximity, but slightly dissimilar, with a mean of 3.83 and a standard deviation of 2.59, again reflecting divergence across the sample for this pairing. Furthermore, Detection systems, as a concept was an outlier within this cluster, but was considered related to Crime prevention with a mean of 2.43 and a standard deviation of 1.79. The inclusion of detection systems within this cluster is interesting as it was also considered close to defence in depth, with a mean rating of 1.64 supported by a standard deviation of 0.74 indicating strong consensus for this pairing.

5.4.2.2 Cluster Two

Cluster Two displayed further spread than other clusters, with reviewing reports somewhat central within this cluster. Reviewing reports was located very close to electric power; however, their similarity rating was 5.23 with a standard deviation of 2.59. This measure indicated they were considered dissimilar by the sample, and ought to have been separate spatially. Reviewing reports and systems theory were spatially slightly apart within the cluster with a mean of 3.86 and a standard deviation of 2.35, indicating diverging perceptions in their dissimilarity. In addition, reviewing reports and risk were clustered with a mean similarity rating of 2.38 supported by a reasonable standard deviation of 1.26 indicating a degree of consensus for their relatedness.

Reviewing reports and facility contextualization were also visually separated, with a mean dissimilarity rating of 4.64 and a standard deviation of 3.1, again reflecting divergence across participants for this pairing. Reviewing reports and movement control were also considered somewhat dissimilar and visually they were separated but part of cluster two, with a mean rating of 5.69 and a standard deviation of 3.15, again indicating a substantial degree of divergence in perceptions of dissimilarity across the participants. Finally, reviewing reports and communication skills were part of cluster two, although separated visually they recorded a mean rating of 3.19 therefore were considered related with a standard deviation of 2.23 showing a reasonable degree of consensus for this proximity distance.

5.4.2.3 Cluster Three

Cluster Three grouped tighter than other clusters and included the concepts of security, detection, security principles, structural strengths, closed circuit television (CCTV), barriers and as outliers law and target identification. Central to this cluster appeared to be detection. Detection was considered closely related to security with a dissimilarity rating of 2.00 and a standard deviation of 0.78 indicating strong consensus for this pairing. Detection and structural strengths were visually located in close proximity, yet their mean dissimilarity rating was 5.36 with a standard deviation of 3.15, indicating a high degree of dissention across the sample for this pairing. In addition, detection and

security principles were considered closely related with a dissimilarity rating of 1.79 and a standard deviation of 0.89 indicating strong consensus for this pairing.

Detection and barriers also indicated a degree of separation with a mean dissimilarity rating of 3.71 and a standard deviation of 2.3, yet were visually located in close proximity. Detection and CCTV were located in close proximity and were considered highly related across the group with a mean dissimilarity rating of 2.00 and a standard deviation of 1.24. Detection and target identification were distal visually yet considered related, with a mean dissimilarity rating of 2.5 supported by a standard deviation of 1.99. Detection and law were spatially separated, which was supported by their mean dissimilarity rating of 5.21, however, again the participants indicated divergent perceptions of dissimilarity with a standard deviation of 3.09.

5.4.2.4 Cluster Four

Cluster four included the concepts of defence in depth and delay, with a mean dissimilarity score of 1.36 suggesting the concepts were highly related, with a standard deviation of 0.5 suggesting consensus was strong for this pairing by participants. In addition, defence in depth and safes and vaults were considered highly related with a mean of 2.79, however, the standard deviation for this pairing was 2.35, suggesting a small divergence in perceptions across the sample. Defence in depth and lighting were also considered highly related with a mean of 2.79 with a reasonable degree of consensus across the sample as the standard deviation was 1.89. The cluster also included defence in depth and fire protection with a mean dissimilarity rating of 3.4, and a standard deviation of 2.9, indicating a spread of thoughts in terms of similarity across the sample. Defence in depth and door furniture was another pairing within the cluster, with a mean of 3.86; however, again divergence emerged in perceptions of similarity with a standard deviation of 3.86. Within this cluster a review of door furniture and delay also shows a close relationship, even though door furniture appears further from the main cluster, the mean dissimilarity rating was 1.57, supported by a standard deviation of 0.76 indicating that participants strongly agreed that these two concepts were highly related.

5.4.2.5 Cluster Five

Cluster five was a small clustering of response and planning and design as it was visually separated from clusters two and four, yet sat on the dimensional border between these two clusters. Response and planning and design were considered as similar concepts, with a dissimilarity rating of 2.57 supported by a standard deviation of 1.09, indicating consensus across the sample for their relatedness. Nevertheless, response and defence in depth (Cluster 4) were considered related with a dissimilarity rating of 1.71 and a standard deviation of 1.41, indicating these concepts are considered close in proximity across the sample. In addition, planning and design and defence in depth were also considered closely related with a dissimilarity rating of 1.71 supported by a standard deviation of 0.83.

5.4.3 Dimensional interpretation

Informed by the writings of Davies and Coxon (1982, p. 6) the study also drew on an analysis of the dimensions (Figure 5.4). Dimensional analysis aimed to understand the broader spatial relationships between individual concepts and clusters, as the dimensions defining the space are premised to represent the main properties along which concepts within the domain are organized (Gonzalvo, Canas & Bajo, 1994, p. 601).

The work of Schiffman, Reynalds and Young (1981, p. 253) highlighted that when interpreting the stimulus space the researcher can relate the results to a specific theoretic model. As such, defining the dimensions of the MDS solution represented mathematically in Table 5.13 and graphically in Figure 5.4 was achieved through an analysis of the results of Phase One and Two as well as the literature informing the study (Chapters 2 & 3).

The dimensions were analyzed and labeled as Diagnosis and Treatment accordant with the work of Abbott (1988, p. 40) (Section 3.3) who articulated that professional knowledge is focused towards three salient tasks of practice: diagnosing, inferring and treating. Abbott conceded, however, that inference is often included in the diagnostic process unless a problem is particularly complex and so inference was not included in this two dimensional model. This view was also evident within the context of the extracted category data with physical security as a jurisdictional domain being concerned with the diagnosis, inference and treatment of security or loss-coupled risk concerns manifested through unlawful access or criminogenic enablers in the protection of people, information and property.

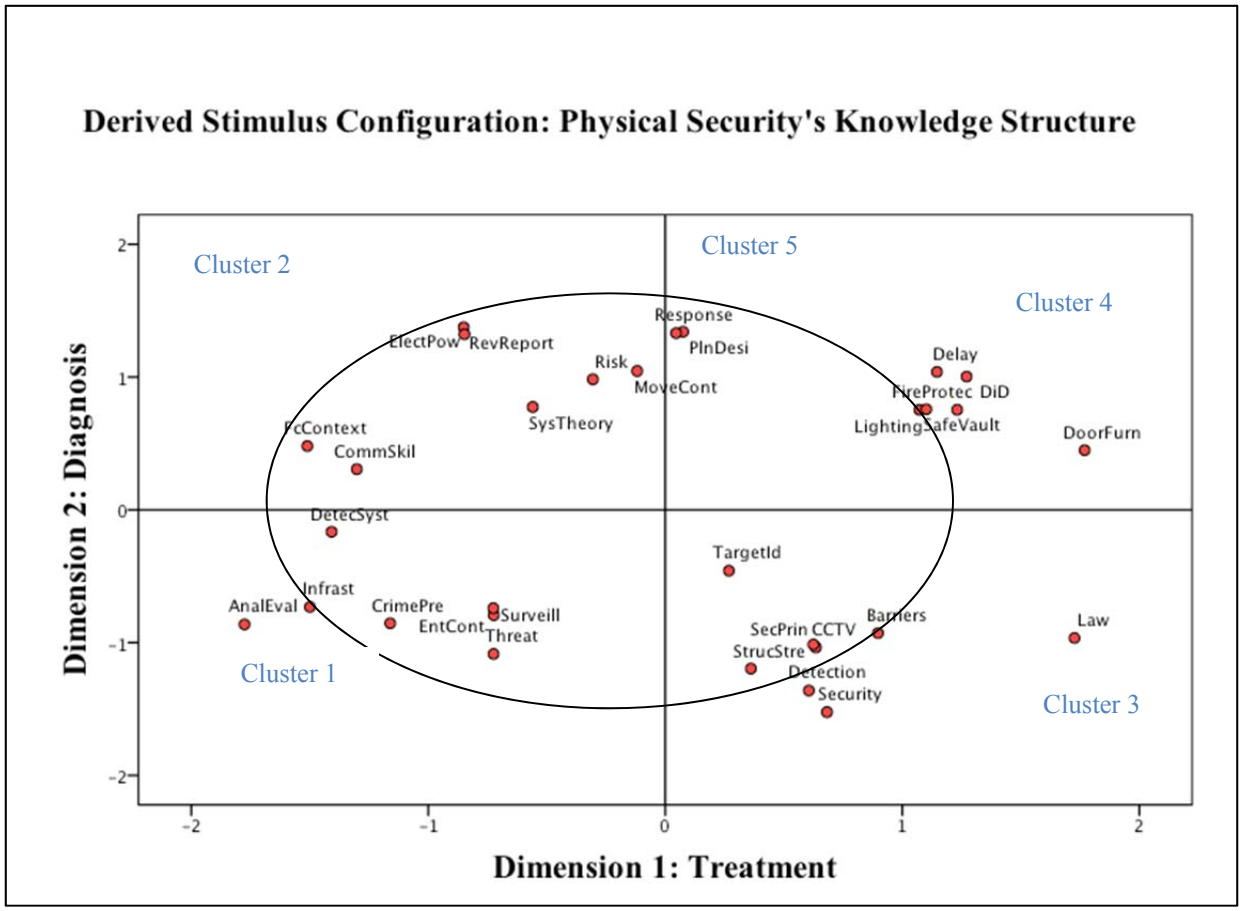
For instance, in the security domain, the professional task of diagnosis was expressed as security risk management and its associated tasks. Subsequently the treatment included the use of physical and technological measures combined with procedural processes that as integrated components provide a physical protection system (PPS).

The PPS components combine to sequentially deter, or detect, delay and respond against, or facilitate recovery from security events. Systematically they reduce opportunities to offend or provide a greater level of difficulty to overcome through their design facets and processes (Section 3.3). Therefore accordant with the work of Davies and Coxon (1982, p. 6) a quasi-circular dimensional space was utilized for interpreting this aspect of the MDS analysis. The quasi-circular dimensional space is argued to represent the tasks of diagnosis and treatment, with inference sitting in dyadic relationship between these two elements accordant with Section 3.3.

Table 5.13 MDS physical security dimensional data

Item No.	Item Name	Dimension 1 Treatment	Dimension 2 Diagnosis
1	Security	.6823	-1.5232
2	PlnDesi	.0750	1.3412
3	DiD	1.2313	.7540
4	Response	.0455	1.3311
5	DoorFurn	1.7691	.4489
6	DetectSys	-1.4080	-.1653
7	Law	1.7263	-.9658
8	Infrast	-1.4994	-.7315
9	Crime pre	-1.1607	-.8540
10	StrucStr	.3609	-1.1956
11	AnalEval	-1.7756	-.8628
12	CommSkil	-1.3018	.3065
13	Barriers	.8974	-.9281
14	Safevaul	1.0721	.7526
15	FireProt	1.2713	1.0039
16	FcContext	-1.5105	.4803
17	MoveCont	-.1186	1.0457
18	RevRepor	-.8507	1.3756
19	Threat	-.7245	-1.0959
20	SysTheor	-.5593	.7744
21	Detectio	.6054	-1.3606
22	Lighting	1.1011	.7578
23	ElectPow	-.8477	1.3223
24	CCTV	.6351	-1.0357
25	Risk	-.3056	.9837
26	Secprin	.6247	-1.0148
27	Delay	1.1460	1.0389
28	Surveill	-.7236	-.7939
29	EntCont	-.7256	-.7409
30	TargetId	.2681	-.4587

Figure 5.4 Physical security's knowledge structure in two-dimensional space



5.4.3.1 Dimension One Treatment

Dimension One of the MDS analysis was considered more related to the notion of problem treatment. As such, it was deduced that higher scores relating to this dimension are indicative of that category area being saliently focused towards the professional practice of security risk treatment, and would therefore be located numerically higher along this scale. This is supported through Table 5.14, which presents the five uppermost correlational scores for this dimension.

Door furniture (DoorFurn) was rated as the highest treatment knowledge category. In Section 5.2.5 door furniture was considered as subordinate to movement control, and superordinate to locks. Door furniture was said to include fittings such as the hinges, hinge bolts and locks (Peter); along with other fittings used on doors to secure building openings for the purpose of restricting unauthorised entry into a protected area. This

treatment element represents one of the most common means of securing an asset, where it was acknowledged in Section 3.1 that evidence of such means of achieving security date back to Egyptian tombs. Accordingly, this is a very accepted treatment option and its N-dimensional place along with its rating as the highest treatment element is logical.

Table 5.14 Treatment dimension

Dimension 1	
DoorFurn	1.7691
Law	1.7263
FireProt	1.2713
DiD	1.2313
Delay	1.1460

The second highest rating for treatment was the concept of law (Table 5.14), and this could be due to the point made by the American Institute of Architects (2004, p. 2) that safety aspects of a building are addressed by building codes which establish minimal standards. Whereas decisions about security are left to the discretion of building owners stating, "it is for the owner to assess security threats, determine risks, and set final priorities for security aspects of a project" (p. 19). As the work of Sarre and Prenzler (2009) allude to in the Australian context, the legal system is more interested in the reasonable treatment of security threats according to the principle of duty of care, often only post event, unless mandated by context, which would then fall into compliance. Eburn (2005) highlights this principle, duty of care, relates to a duty to act reasonably in the circumstances, accordant with the principles of Donoghue v Stevenson. Where Lord Atkin said that we owe a duty of care to our neighbor and for the purposes of the law, our neighbor is:

> Persons who are so closely and directly affected by my act that I ought reasonably have them in contemplation as being so affected when I am directing my mind to the acts or omissions which are called in question. (Eburn, 2005, p. 38)

Eburn (2005, p. 38) highlights that if a reasonable person would realize that what you are planning to do, or not do, may affect a particular person, or class of persons, then you may owe a duty of care to that person or persons Accordingly, risk treatment

options including security risk treatment must be considered reasonable, and it is this aspect that the law is most interested in, rather than problem diagnosis, as owner's treatment of risk must be considered reasonable for the context. As Tooma (2008, p. 2) expresses, in practice safety, security, health and environment risks are managed through management systems, which are underpinned by a risk management methodology.

The third highest knowledge area for treatment was fire protection (FireProt), which is a control measure (treatment) mandated in building codes (American Institute of Architects (2004, p. 2), and is subordinate to law, and subordinate to the thematic category of detection systems, representing another important and common operational element of built environment risk treatment.

Defence in depth (DiD) was the fourth highest treatment category, which was considered subordinate to crime prevention (Section 5.2.5) but superordinate to its embodying element categories of detection, delay and response. Thus accordant with Section 3.3, Defence in depth as a security theory represents a foremost methodological means of treating security risk concerns. The fifth highest treatment category was barriers, which again are often a salient means for treating unauthorized access risk concerns. Therefore its rating as a salient means of risk treatment is also logical. As the American Institute of architects (2004, p. 4) point out, "the most obvious protection from the effects of a hostile act is any barrier that can prevent or delay an adversary from reaching a target…Generally, physical security may be seen as a means of providing more time to ensure safety" (p. 13). Such a focus on barriers as a means of delay is congruent with the rating of barriers as a dominant treatment knowledge category for physical security professionals.

5.4.3.1 Dimension Two Diagnosis

Dimension Two related to the notion of problem diagnosis and as such higher scores relating to this dimension are indicative of the knowledge areas being saliently focused towards the professional practice of diagnosing security risk concerns. Table 5.15 shows that for this dimension reviewing reports was the highest rated category. Reviewing reports was considered significant for understanding the security or crime problem to be

addressed and was deduced as subordinate to planning and design and infrastructure. It was acknowledged that for many security professionals the ability to critically review documentation is essential in order to establish the security risk context, prior to treatment planning.

Table 5.15 Diagnosis dimension

Dimension 2	
RevRepor	1.3756
PlnDesi	1.3412
Response	1.3311
ElectPow	1.3223
MoveCont	1.0457

Planning and design was the second highest diagnosis category, yet was also located dimensionally as high in treatment, perhaps due to the interrelationships with all other aspects of security problem treatment, as planning and design is a very broad term. It is logical that without clear planning, problem articulation is not possible; however, the design aspect of this category could also be considered a treatment element. This may explain why this broad term sits numerically high in terms of diagnosis, but is dimensionally located as a treatment.

Furthermore, Response was the third highest diagnosis category in terms of problem definition. This is perhaps due to the role of detection and delay in providing enough time to facilitate the response plan (Garcia, 2001, 2009), and therefore many security professionals approach their security planning cognizant of this. Consequently many security professionals want to understand the response aspects and then work backwards, articulating the detection, and delay elements accordant with response planning. As Garcia (2001) explained, detection must occur before delay in a PPS, and the delay time after detection must exceed the response time for the system to be effective. It is acknowledged that physical security aims to provide a means of delay, after detection to facilitate a response. Therefore, one means of articulating the amount of physical security (diagnosis) is to understand the delay time required in relation to response, as delay measures are expensive.

Electric power (ElectPow) was another diagnosis means, and this is perhaps due to the dominance of electronic security measures used to achieve functional security in

contemporary times. Movement control was the fifth diagnostic knowledge category; a broad conceptual security category, which directly relates to a core principle of physical security, to control access to protected assets and also egress from facilities. This category is superordinate to Barriers and Door furniture, and other content areas such as walls, fences, windows and glass. Thus, understanding the requirements to control movement is a major diagnostic aspect of risk treatment.

5.4.4 Phase Three: Interpretation

Phase Three of the study sought to respond to the research question:

What is physical security's knowledge content structure as measured by multidimensional statistical scaling?

Phase Three, through Figure 5.4, highlights that physical security's knowledge content structure relates to clusters of knowledge categories and subordinate concepts circularly banded, then dimensionally organized around the professional tasks of diagnosis, inference (reasoning about) and treatment of contextual security or crime prevention problems. These problems relate to the manifestation of harm to people, information or property through malicious actors achieved through unlawful access or crime enablers (Section 3.3). Figure 5.4 provides an iterative blue print for establishing a knowledge or curriculum framework for physical security professionals indicating, for curriculum ordering purposes, that physical security's knowledge content should be presented and taught in a manner that reflects these professional tasks.

5.5 Phase Four: Expert focus group

5.5.1 Physical security knowledge evaluation

Phase Four incorporated a qualitative analysis of a focus group interview, from a purposive sample of security experts (n=4), utilizing a discourse analysis. This phase drew on the writings of Barnett (1994, p. 46) who articulated that the identification, selection and ordering of identified knowledge elements along with supporting learning outcomes represents an epistemic framework or curriculum.

Phase Four sought to understand the knowledge content and structure identified in previous study phases, within the context of an ideal curriculum for future physical security professionals. As such, in response to Phase One, Two and Three outcomes (Figures 5.2, 5.3 & 5.4), Phase Four sought to respond to the question: what are the learning objectives and knowledge requisites for physical security professionals as an organised knowledge system?

5.5.1.1 Participants

Four security experts were included in the focus group: Dave, Jeff, Cliff and Kevin. Their profiles can be viewed in Table 5.16.

Table 5.16 Phase Four: Expert profiles

Name	**Profile**
Dave	A security educator with 33 years of experience within the security domain, having been employed in the Military, Corporate Security and Private Security sectors. Qualifications include a PhD, Masters by Research, Bachelor of Science, an Advanced Diploma in Engineering and trade certificates. Dave has presented research works at numerous security conferences, as well as publishing over 18 International Journal articles, five book chapters and four books in the area of security and security science.
Jeff	A former army officer who served in a variety of security and intelligence roles over the course of his career. After serving 20 years in the military Jeff moved into the precious minerals resource sector, concentrating on meeting the security intelligence needs of this sector. Jeff currently works in academia where he coordinates and teaches in the area of intelligence and terrorism at an Australian university.
Cliff	Consultancy focus includes the design and analysis of physical protection systems, security risk analysis and security risk management for strategic facilities, the security of national infrastructure facilities, and the application of access control systems and intelligent CCTV. Qualifications include a BSc (Applied Science), Graduate Diploma in Applied Science, Master of Applied Science (Physics), Doctor of Philosophy, Teachers Certificate, and a Teachers Higher Education Certificate.
Kevin	A Primary consultant and the Security Risk Team Leader in a Western Australian annexed Central Building Engineering group. Kevin's qualifications include, a Doctor of Philosophy (PhD) (Security Science), Bachelor of Science (BSc) Honours, (computer Science). Kevin is also a Certified Biometrics Professional. Kevin also has a background in research and development, having published his security research in the world's highest ranked peer-reviewed Optics Express Journal, and presented at national and international security conferences.

5.5.1.2 Administration of focus group

The focus group interview took approximately one hour, and comprised questions (Table 5.17) to guide the phase outcomes (Appendix C). The questions sought participant's thoughts relating to requisite knowledge and teaching structure within the domain of physical security accordant with their professional experience and supporting learning objectives. It also sought their final opinion of the knowledge structure, and provided them the final opportunity to recommend adjustments to the hierarchical table and supporting heuristic.

Table 5.17 Phase Four: Expert focus group questions

No.	Interview questions
1	What is the higher education learning objective/s for a physical security professional?
2	In terms of articulating a formal knowledge system, based on these maps what do you see as the foundation content requirements to be learned by physical security professionals before qualification?
3	Higher education students should learn or know the science or knowledge of which their future domain is built. Based on this view, what is the scope of higher education knowledge?
4	How should these units be organized?
5	Do you believe these maps capture the knowledge concepts required for a physical security professional?
6	What are the strengths and perhaps weaknesses of these maps in terms of establishing a physical security professional's knowledge system?

5.5.2 Focus group analysis

This phase highlighted that the knowledge requisites for a physical security professional include core security concepts along with the sciences and models of learning (social sciences) that underpin them, as well as the supporting academic skills that are professional enablers within a protective security or crime prevention role. As Kevin expressed, it is important to keep the end game in mind; stating:

> I actually hired a graduate from a university security terrorism and counterterrorism course, and his learning units did not relate to his tasks occupationally, the course materials must relate to the professional tasks. (Kevin)

During this phase Dave expressed that in terms of identifying knowledge unit requisites to be learned by physical security professionals before qualification, "it is what you've got listed here (Tables, 5.6, 5.7 and 5.8, and Figures 5.2, 5.3 and 5.4), but at a more restricted level though". However, Dave also noted that foundational elements such as strength and materials, physics, should be included stating, "they need to understand these aspects, understand the limitations, so when they go to the structural engineer to formally do the final calculation they understand it...but this is missing from the tables".

This phase acknowledged that most security professionals are not generally engineers. Acknowledging this, Jeff voiced that the role is focused towards the diagnosis and then the selection and implementation post diagnosis of those appropriate physical security elements that go into the security system or program, not actually putting them together. Therefore the scope of their professional education is diagnosis of the problem and articulation of controls (treatment), not assembly expertise; although they may hold this.

As Jeff expressed:

> The ability to diagnose is critical, so each of those elements that allows them to diagnose the problem is what they need to have as a graduate, along with graduate attributes of communication, research and the like, because at the end of the day if they can't diagnose the problem, they are no use to anyone. (Jeff)

In terms of fundamental knowledge the group considered that the knowledge tables and heuristics accurately captured the salient occupational knowledge for a physical security professional. As Kevin noted, "they have got the main ones". Nonetheless, some category areas did raise critical discussion. For instance, the inclusion of fire protection raised questions. However, it was explained that as a knowledge area this kept occurring in the literature extraction. To this point Kevin, responded "that's right, we need to know the fundamentals, but I was just wondering how you got it in here". Jeff made the comment that "security is about protection, there is a logical fit". Cliff also raised the observation that some inputs were physical such as door furniture, whereas others were ideas such as systems theory. This highlighted and formally acknowledged that the knowledge maps sought to understand what the knowledge areas are, and their

relationships. This included theories, concepts and principles based on superordinate and subordinate stipulations, where some inputs sit under category themes as operational deliverables.

In addition, because of concept reduction (Phase Three) some operational elements stayed, whereas some were removed based on word count analysis and Phase Two input. Kevin acknowledged these problems as security wide issues.

> CCTV and risk have their own body of knowledge all together, and I have worked with people who see security as a subset of risk, not the other way around. But physical security professionals, accordant with the research to date, must hold this knowledge as part of their broader body of knowledge, but they may not be specific area experts. (Kevin)

The final category which stimulated considerable discussion was law which could be considered as both a diagnosis and a treatment in many cases. Dave noted that on the MDS map, law is clustered with the treatment elements "more to the explicit type areas, instead of at the more diagnostic". Jeff responded with "You consider law when you get to treatment, but in terms of diagnostic you don't need to give it any consideration…diagnosis can exist without worrying about law".

Jeff's view separated diagnosis from compliance, a view supported in the American Institute of Architects' Security planning and design text. They clearly make the distinction between building safety and security, highlighting that the safety aspect of buildings is addressed by building codes, which establish legally binding minimum standards. However, security decisions are left to the discretion of building owners and their managers and operators (2004, p. 2). Kevin also concurred with this point, highlighting that law is a treatment, and that there is legislation sitting around the use of treatment options such as CCTV. These views are consistent with Section 5.4.2 (Dimensional Interpretation).

An analysis of the group's discussion saw the foundational knowledge emerge as per the outcomes of the earlier phases of the pilot study. Knowledge was seen as saliently focused towards the diagnosis of the problem and articulation of treatment elements, but

not necessarily expertise in their installation and operation, as accordant with Abbott's work these may be delegated to other workers. This is congruent with Figure 1.1 of the study, which saw the security professional sitting above the occupational category operators such as alarm installers who undertake the assembly and maintenance roles yet sit subordinate to the security professional. However, it also highlights a limitation with this Figure (1.1) as the physical security professional would also sit parallel with, rather than above, other professionals undertaking their part of the risk treatment process such as engineers.

Furthermore, Cliff made the point that these knowledge units must epistemically be organised hierarchically in terms of skills, stating:

> It's got to be in terms of skills, hierarchy of skills, so define the skills as needed in a particular unit of study…the skills will be cognitive skills, but they could also be application skills, but in a higher degree, you would expect them to be cognitive skills in the main. (Cliff)

From an educational standpoint elements should be organised and taught in terms of a combined science and arts (social sciences) approach to diagnose first and then treat security concerns, ordered based on prior knowledge competencies, as per Table 5.10 and Figure 5.2. Furthermore, the scope of learning concerns the relationships between knowledge areas, how each knowledge category or unit fits systematically with the others to provide a sound diagnosis and optimal treatment strategy. Therefore the scope of security higher education in this context needs to focus on the relationship between concept units and the arts and science underpinnings on which their future domain is built. For example, Dave articulated "there has to be a strong relationship between concepts, basically what you are doing (tables and figures), so where does CPTED fit into physical security, where does physical security fit into threat, and that sort of relationship knowledge"?

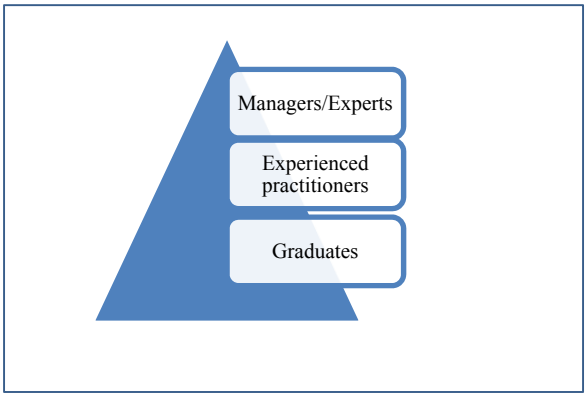
This analysis highlights that the epistemic scope therefore relates to teaching the systematic structure of the domain, the purpose or aim of individual knowledge category areas, along with their underlying sciences and how individual knowledge category areas fit together with other areas to achieve the desired outcome. Participants

believed that students need to learn core knowledge within their domain to practice however recognised that as graduates there is a need for further development. That is, once students separate from educational institutions and go into professional practice, moving into their employment context streams they then learn more focused skills.

This discourse highlighted that after graduating and gaining practical experience with their core knowledge, graduates need to learn additional higher-level management skills, such as those taught in a Masters of Business Administration (MBA). For instance, Dave made the point that, "they learn very high technical skills, then, as they progress they move into more of a business management role". At this stage the interviewer confirmed, "so we leave the management knowledge to much later and teach the technical skills that they practice first"? Dave responded, "yes, but when I say technical skills I am referring to risk management, business continuity, all those (categories), not technology".

Kevin agreed with Dave's view, emphasising that his role is managerial with a focus towards bringing in work and overseeing and quality controlling outputs. He further noted that his subordinates' roles are focussed on systems analysis and development in terms of physical protection systems. Such a view introduced a stratum within the security professional's group, specifically for those working in large multinational organisations. At its core, this strata hierarchically includes graduates, experienced practitioners and managers or experts (Figure 5.5). However, consultants working for themselves logically must be within some level of this strata, either as experienced practitioners or specific area experts.

Figure 5.5 The security professional's stratum



The pilot study also sought interim learning objectives for physical security professionals graduating from university programs. A focus on university-level study is vital given that it is recognised by the literature, the broader public and indeed the legal arena that this is the minimum requirement for a professional study program in an Australian context. In response to this Cliff raised a maturation concern at the undergraduate level and drew on the University of Western Australia's (UWA) medical program as an example, stating:

> In first year undergraduates do not touch a medical laboratory until their second year. First year is in fact first year science, chemistry, physics biology and whatever else, in order to give them some maturity…is that an issue for physical security? (Cliff)

This point leads back to the notion of subject ordering with the emphasis on learning the science that underpins the professional domain and allowing for a process of maturity for school leavers. Informing the learning objectives for graduates, it may be that the underpinning sciences for physical security ought to be taught in the first year of a learning program (sequencing). With this in mind Dave expressed that for the higher educational learning, the key objective we want them (students) to get out of a university education is the systems approach, stating:

> So they understand the components that make up the individual elements of physical security, and how those systems integrate and that foundation of knowledge. However, when you say broader goals, it comes back to you are trying to bound this into physical, so do they need to understand risk, do they need to understand business continuity, do they need to understand communication? (Dave)

However, Jeff pointed out that if focusing purely on the physical security, then he would be looking at engineers. Acknowledging such views, deference was made to the definition of physical security; as a device, system or practice of a tangible nature (Section 3.1). Therefore physical security practices would include the technical, physical and procedural elements of the system. A view supported by Kevin who added that in professional consultancy he does not separate physical security from the other

functions of security risk assessment, threat assessment or vulnerability assessment, "I try to do all as one exercise". Kevin's comments highlight the necessity for physical security professionals to understand the purpose or drivers. At this stage the researcher drew their attention to the knowledge tables and heuristics and made the statement that this very notion is encapsulated in the extracted knowledge system, stating, "So when you talk about diagnosis, the diagnosis is security risk management". Kevin responded with a statement emphasizing his point:

> To take a very simple example, there is a camera outside of this room, so if you gave the plans of this building to an electrical engineer and said please give me CCTV coverage; what thought process will that electrical engineer go through to put a camera outside of this room, and what would be the different mindset and thought process if you gave the same task to a security consultant or a security science graduate? (Kevin), "So you are looking at the broader problem solving process in relation to the context" (Interviewer)? Yes. (Kevin)

This was a view agreed to by Cliff, highlighting that learning objectives in higher education reflect attributes such as independent learning and problem solving stating "these I reckon are higher education learning objectives". Jeff added:

> It comes back to the general attributes, and the discussion we've had previously about the significance of graduate attributes, that are generic attributes for the university such as ethical thinking, diagnostic thinking, communications, all of those basic things…those core graduate attributes actually apply in all professional domain spaces. (Jeff)

Directly responding to Jeff's view, Cliff stated, "I'd say that is a good starting point". This point in the focus group highlighted that security professional's learning objectives must include those general academic attributes embedded in all higher education courses, such as the ability to problem solve, communicate and so on. These are embedded into learning the underpinning sciences that the domain practices. As Jeff states:

> I think back to my domain space of intelligence, we don't care what the specific qualification is, it is those core attributes that we are actually interested in, and the fact that the graduate is in the top percentile of all other graduates…As this means they can adapt to whatever environment we put them in. (Jeff)

> "So you are saying the learning objectives remain the same, but it is within that context of diagnosis, inference and treatment of physical access problems"? (Interviewer)…

> Yes…an outstanding intelligence analyst is the one that can communicate his diagnosis to the decision maker and get an appropriate decision made; whereas, the person who can understand the theory and understand what the problem is, but cannot communicate that effectively to somebody to make a decision, then they are a complete and utter waste of time. (Jeff)

Dave's views took the position that learning objectives need to focus on outcomes from technical knowledge, stating:

> Where you sit vertically in your organization will define what you want as a learning objective, plus what you want to get out of any education. At the lower level as a graduate there is a lot of high technical skills, whereas as you sort of move up it becomes about higher management, and communication, and you don't need those technical skills because you are managing a broader group. (Dave)

Jeff supported this view interjecting,

> A doctor goes out and becomes an intern, an accountant goes out and becomes a junior accountant, a manager goes out and becomes an advisor or something like that, they go into graduate jobs and then they progress upwards, but security does not do that…the profession needs to have staged hierarchically that allows them (employers) to take graduates and develop them. (Jeff)

This discourse highlighted the need for learning objectives to include professional knowledge and skills required for entry-level positions, on which a graduate can develop further expertise through experience and professional mentoring. Further guiding the development of physical security learning objectives was the recognition of professional accreditation, and where a university program should end and other training be pursued. For instance, Jeff stated, "in other professions the degree is only the first step, you've got to get registration within that". Dave acknowledged Jeff's point, stating that "registration is professional development…but such development does not give the foundation", that is education's role.

Dave expressed "I know it's probably not a learning objective, but they [students] need to know the elements that make up a system and understand how to apply those elements". Cliff considered this to emphasize content rather than an outcome, stating, "that is content structure though". Dave acknowledged Cliff's view stating, "yeah I know, otherwise the learning objective becomes an abstract - good communication, ability to work in teams focus". Dave considered that from a learning perspective students must be given the technical skills of what physical security professionals need, for example, CPTED, Defence in depth, Path analysis, all the elements, and how they go together. The interviewer responded, "so you need to expose them to the depth and breadth of that theory as it relates to the domain area"? Dave responded, "yes, what is a PIR, the physics that underline PIR and how PIR fits into the system, and how you are going to contextualize it". Kevin added:

> Yes…but this is technical knowledge, at the end of the day you are giving a person a report, and so you can be very good technically, but your report writing skills also have to be excellent as well. That is something that I see lacking in some people coming out of universities. (Kevin)

5.5.3 Phase Four: Findings

Phase Four of the study sought to respond to the question: *Based on the extracted knowledge system; what are the knowledge requisites and supporting learning objectives for physical security professionals*?

Nevertheless, an exact learning objective or set of learning objectives was not provided by the panel. However, an analysis of their discourse lead to an understanding that the learning objectives for future physical security professionals must relate to teaching the knowledge content areas and structure uncovered throughout this study as represented through Tables, 5.8, 5.9 and 5.10, and Figures 5.2, 5.3 and 5.4. Additionally there was an emphasis on understanding the uncovered epistemic relationships: how each knowledge category or unit fits systematically with the others to provide physical security outcomes.

Phase Four emphasised that a knowledge system for future security professionals should be a combined science arts approach due to the broad scope of the domain and the breadth and depth of its knowledge base. The knowledge sitting within this system relates to diagnosis, reasoning about and treatment of contextual physical security or crime prevention problems These provide the why and how in terms of problem solving for security diagnosis and treatment; how this knowledge is applied for physical security related concerns. Furthermore, this learning must be underpinned by traditional academic attributes such as communications skills, analytical ability, capacity to work in teams and so on. It is argued that such learning underpins a future professionals' ability to work with others to diagnose, reason about (infer) and deduce treatment options accordant with the physical security context.

The nature of professional work was addressed during this phase where it was supported that security professionals do not need the capacity to undertake installation and operational work. Rather, it was acknowledged that security professionals must understand theoretically how individual treatment measures work, and how their integration achieves an optimal treatment strategy and be able to prescribe the most appropriate strategy for the context. This highlights important behavioural outcomes necessary for physical security professionals and the importance of a graduate's capacity to apply academic knowledge.

Consequently the learning objective for a physical security professional could be specified as a combined cognitive and behavioral outcome, For instance:

> Apply an educated body of knowledge to diagnose physical security requirements for a facility, and develop a logical treatment plan (system) attuned with control measures underpinning sciences, and communicate this evaluation verbally and in writing.

Nonetheless, this can only be considered an inferred learning objective, as the group was unable to directly articulate this. Therefore, such an assertion needs to be tested in the primary study.

Irrespective of the learning objectives associated with university programs the group acknowledged the importance of ongoing development and professional mentoring post-qualification for graduates to progress in their career and their capacity to be expert physical security specialists.

5.6 Interpretation: Can the study meet its objectives?

The reviewed literature highlighted that to date an explicit formal body of knowledge showing content, structure and relationships for institutions of higher education does not exist for the domain of physical security (Section 3.9). Such a dearth of understanding exists in light of the reviewed works of Abbot (1988, pp. 52-54), Wilensky (1964); Eraut (1994), Griffiths, Brooks & Corkill (2011) and Freckelton & Selby (2013, Chapters 2 & 3), which emphasise that formal academic knowledge legitimizes professional work. Therefore steering the interpretation of the pilot study's data is the works of Eraut (1994, p. 103) and Griffiths, Brooks and Corkill (2011, p. 3) which combined emphasize that such understanding (higher education curriculum) is based on maps of propositional knowledge that are both theoretical yet functional. Such maps include both content and structure, emphasising systematic connections (Bruner, 1977, p. 2) that are hierarchical or organised in some other way, but force the expression of broader themes, and tie the specifics together (Posner & Rudnitsky, 1982, pp. 8-39).

The feasibility of this study is based on the ability to link its individual phase outcomes to the study's overarching research question: *What is a desirable knowledge system for physical security professionals as conveyed through the published literature and accessible professionals*?

Phase One of the study sought to develop an initial cultural map of the key concepts and organisational structure of relevant knowledge within the domain of physical security. Using three printed texts, a count analysis was undertaken to identify key themes. These themes were then hierarchically ordered using a process of deductive analysis. During Phase Two, physical security experts, validated these knowledge frameworks (Tables 5.4, 5.5 and Figure 5.1) developed in Phase One and provided additional input and enhancements in the context of a semi-structured interview. The final outcomes of this stage were a list of key concepts (Table 5.9) identified through the initial literature review as well as additional concepts provided by the experts not uncovered previously. These key concepts were structured hierarchically and presented in Table 5.10 and Figure 5.2. Accordant with the work of Krimsky and Golding (1992, pp. 9-10) (Section 3.10) Table 5.10 and Figures 5.2, 5.3 and 5.4 offer a conceptual net or template of cultural order and structure towards making the knowledge system explicit, or more conscious.

Phase Three saw the salient knowledge concept categories tested for macro-structure using multidimensional statistical scaling. This process provided an objective analysis of how concept categories are related. The outcomes of this procedure supported the cultural taxonomy developed via Phase One and Phase Two. The MDS analysis also highlighted the broader dimensions of diagnosis and treatment of security concerns within the physical security knowledge corpus.

Through discourse analysis using a focus group, Phase Four sought validation of earlier phases as well as articulating an ideal higher education curriculum for security professionals. Research participants agreed that the knowledge maps presented in Tables 5.9 and 5.10 along with Figure 5.2, derived through the study's methodology, represented a desirable body of knowledge for physical security professionals, providing clarity and coherence concerning what is to be taught (see Section 3.10) for professional practice before qualification.

Thus an ideal curriculum, based on the knowledge frameworks would provide a mixture of core theories, concepts and practice principle content areas for the domain of physical security. Core concepts include the very concept of security, along with the concepts of surveillance, risk, law and crime prevention. Also included are core theories such as

Defence in depth and crime prevention through environmental design. These are supported by core practice principles such as detection, delay and response principles, and their underpinning occupational means. Also included are general security principles including entry control, facility contextualization, and target identification along with fire protection. These are further supported by occupational practice components such as security lighting, safes and vaults, detection systems, door furniture systems, and electric power delivery.

Pilot study findings stress that such core domain knowledge is fused with general academic concepts, theories and professional practice principles, which combine to produce a graduate's system of knowledge. These included analysis and evaluation as general concepts employed in all professional practice domains. Then systems theory was found to be a general academic theoretical frame essential for achieving a professional security solution. This knowledge was further supported by general professional practice principles such as planning and design and understanding synergies across infrastructure. These were further braced by professional occupational practice elements such as the ability to clearly communicate, verbally and in writing, along with the capacity to critically review reports.

The pilot study supported that a desirable knowledge system for physical security professionals can be developed applying the study's methodology. The system of knowledge captured through the pilot study led to the development of a number of body of knowledge assertions to be tested in the primary study.

1. Heuristics representing the propositional knowledge and distinct networks of relations amongst the various theories, concepts, principles and practice components or elements for physical security professionals can be developed for enhancing reception learning;
2. A desirable knowledge system for physical security professionals relates to core foundational physical security and crime prevention knowledge, braced by general academic knowledge that underpins professional work;
3. The course learning objective and therefore educational goal for a physical security professional can be represented as: an ability to apply scientific knowledge and critical thinking techniques to diagnose physical security or crime prevention

requirements for a risk context, and develop a systematic treatment plan and communicate their evaluation to clients; and

4. Physical security education needs to include both a science and arts approach to include the physical and social sciences that underpin the higher strata tasks of the professional domain.

These assertions include the foundational technical knowledge (the science or learning) that makes-up or underpins each discrete yet interrelated area, and that formal articulation and acknowledgement of the science and learning precedes the professional label. For example, Table 5.9 presents the knowledge category or risk, where according to Talbot and Jakeman (2009, p. 130) risk arises out of uncertainty (p. 130) and risk can be conceptualised qualitatively through descriptive terms, or quantitatively through mathematics.

To understand risk, security professionals need to understand it quantitatively and descriptively, and therefore require both qualitative analysis skills along with mathematical comprehension to conceptualise risk and communicate messages accordingly. Thus, mathematics is a subordinate concept of risk, therefore security professionals must understand how to evaluate risk using historical or calculated data (p. 143). In addition, detection technologies work of physics principles and therefore security professionals must understand the physics that underpins these technologies in order to employ them appropriately. As Cliff said, “we need to hammer home this point”, thus in the engineering approach physics is a supporting area of detection technologies which needs to be taught to an understanding level to physical security professionals.

5.7 Pilot study reflection

Informed by the writings of Martin (2000, p. 136) the pilot study sought to trial the study’s proposed methodology, collection instruments and methods of analysis. In addition, the pilot study also sought to gain an interim understanding of physical security’s knowledge system. Therefore, the objective was to identify and overcome major problems before proceeding with the larger, more resource-intensive primary study.

A major difficulty for the study to address was the language variances used within the security domain. Often many terms can define explicitly different concepts or principles, or communicate the same concept or principles in different ways. This was an issue acknowledged for the security domain in the work of Manunta (1999) and was highlighted in the Phase One literature extraction and Phase Two interviews, and again in the Phase Four focus group interviews. During his interview Peter pointed out (Participant 2) that discussing merged terms in security "is a study in and of itself". Peter expressed the position that, "rather than get too bogged down in the granular details at this stage what you need to do is capture the broader terms and their general understanding to capture an initial body of knowledge which can be refined over time". Brooks (2008, p. 154) acknowledged this issue also in his study of the knowledge domain of security risk management, making the point that the study did not attempt to provide precise concept definition, allowing the experts to define their own understanding through relationship of concepts or knowledge structure. This lead to the view that the exploratory stage of the study would highlight what it is we need to define, whereas the descriptive and explanatory phases would provide the context in which such definitions need to be based.

Exploration of language variations in the security domain resulted in expert interviews taking longer than anticipated with each interview lasting 90 minutes rather than the planned 60 minutes. This issue was raised by Peter who suggested that from a professional's standpoint the ideal time would be around 45 minutes due to work schedules. In addition, participants suggested that it would be helpful to be able to review the interview questions and supporting materials prior to the interview taking place.

To address these concerns in Phase Two of the primary study, interview questionnaire changes were made where participants were asked prior to commencing if any study terms needed to be clarified, and the security lexicon was used if terms were ambiguous to provide clarification. This aimed to overcome some language ambiguity within the study and shortened the questionnaire thus reducing interview time. Further, knowledge system information was sent to participants prior to their formal interviews taking place. While it is acknowledged that not all participants may have reviewed the material it

provided the opportunity for them to do so and as a result, enabled a stronger participant centred analysis.

Methodological changes were also identified for Phase Three. During the data reduction CPTED was considered subordinate to planning and design and therefore not included in the MDS analysis. This was considered a mistake on reflection, as CPTED is a major theoretical planning consideration for physical security and crime prevention. Therefore, in conducting the data reduction in the principal study attention will be towards the quantitative concept results, and where salient numerical representation found, the concept or theory retained for the MDS analysis. This also applied to the merging of synonymous terms, where Detection was merged with alarm systems which was supported in Phase Two interviews, yet on reflection detection is a broader concept and the alarm system is a functional means to achieve security and so are separate aspects in the body of knowledge.

The MDS questionnaire itself was deemed too long by interview participants. Therefore, as with the writings of Giguere (2006, p. 29) the survey questionnaire for the primary study was broken into two conditions where participants were randomly assigned to respond to a set of questions, distributing the dissimilarity rating for the study over the two survey questionnaires.

A number of changes were also made to the focus group procedure (Phase Four) with the questionnaire and knowledge tables and heuristics sent to participants prior to the focus group taking place. In addition, the order of questions was changed to reflect a building process in participant responses. This included moving question one, "what are the higher education learning objectives for future physical security professionals" to question 8, being the last question as this proved difficult to respond to as a first question in the pilot study.

Finally, focus group participants gave input regarding the selection of expert participants for the primary study. There was an acknowledgement of a stratum of professionals in the security industry including graduates, competent professionals, senior managers and experts (Figure 5.5). Pilot study participants suggested including professionals working in the 'competent professional' strata or as direct physical

security consultants as these would be most up-to-date with regards to technical skills. It was suggested that graduate professionals were still developing and higher managers have a focus towards different skill sets. The pilot study therefore leads a number of changes to the primary study's methodology and procedures Table 5.18.

Table 5.18 Study methodology and procedures changes

Phases	**Changes**
Phase One	Key words only, excluding phrases were used to extract physical security's explicit knowledge base.
Phase Two	The interpretation and defining of ambiguous categories removed from the study, as per Brooks participants were left to define the terms as they understood them and discussion and clarification offered if requested. The semi-structured interview questionnaire was reduced in size to meet time restrictions for participants (Appendix D).
Phase Three	Phase Two saw the MDS survey questionnaire divided into two questionnaires to reduce the length and time required to complete the survey (Appendix E).
Phase Four	Participants were asked at the completion of the focus group to write down what they believed the learning objectives should be, or relate for physical security education (Appendix F).

With minor changes to data collection instruments and procedures and participant sampling the pilot study supported the mixed methods research methodology as a valid means of extracting physical security's explicit knowledge system and supporting educational objectives. It highlighted that the data extraction and analysis techniques could deliver maps of propositional knowledge representative of that knowledge required by professionals to work in the physical security domain, thus meeting the study's objectives.

5.8 Conclusion

To advance the physical security domain, a cohesive body of knowledge must be identified and then used to develop learning objectives as a basis for university programs. To achieve such outcomes, a complex, multiphase, mixed methods research study, based on constructivist principles, was devised. To test the methodology, research tools and analytical techniques a pilot study was undertaken.

This chapter presented an overview of the pilot study including the pilot study's trial methodology broken into the four discrete phases. Phase One of the study involved a

literature extraction based on three published texts to provide key knowledge concept category areas for the physical security domain which were then hierarchically ordered. In Phase Two expert interviews provided validation and enrichment of the knowledge category frameworks delivered. An MDS analysis of the domain space was conducted in Phase Three further supporting findings. During Phase Four a focus group was conducted to define learning objectives for higher education courses in the security domain.

Initial findings suggest that physical security contains identifiable, consensual, core concept knowledge areas which can be epistemically organised. This body of knowledge can be best taught to students using a science and arts based approach, focusing on the key areas of diagnosis, inference and treatment, underpinned by graduate attributes such as communications skills, working in a team and so on.

As a result of the Pilot Study some minor changes were identified for the Primary Study. Despite this, outcomes from the pilot study suggest that the methodology employed could reliably and validly be used to generate a body of knowledge for physical security and to identify learning outcomes.

Participants were fully engaged with the process and were supportive of the study. As one participant said “the results will be very interesting”. Certainly the results of the study will have significant implications for the professionalisation of the physical security domain.

Chapter 6: Study Phase One: Knowledge category exploration

6.1 Introduction

This chapter presents Phase One of the study, the development of an explicit knowledge corpus for physical security professionals organized hierarchically accordant with local connections between data elements. This phase of the study sought to make explicit physical security's dispersed knowledge system as represented in security specific printed texts. The annotated bibliography data extraction is divided into two security thematic stages, initially presenting text books specifically titled towards physical security and physical protection systems (Stage 1). The second stage analysed broader security texts with an asset protective focus including crime prevention theories, concepts and principles within the non-traditional security domain stream (Stage 2). Combined, this approach sought to capture the salient concepts, ideas, principles, and theories representing an ideal physical security knowledge system. The chapter is divided into discrete discourses demonstrating the building of knowledge based on previous knowledge congruent with the principles of constructivism (Section 1.8).

Section 6.2 introduces the annotated bibliographic data extraction as the means for uncovering repeated themes within physical security's shared paradigm. Then Section 6.3 presents the individual texts' data extractions, commencing with Text One and concluding with Text Fifteen. Section 6.4 presents the concept categories derived from the literature analysis (Table 6.16), combined with expert concept categories carried forward from the pilot study (Table 6.17) to produce a Phase knowledge table (Table 6.18). This table is, through deductive analysis, ordered hierarchically to represent physical security knowledge concept categories and their local relationships (Table 6.19). Following this, Section 6.5 interprets the findings from this phase. Section 6.6 of the chapter acknowledges limitations within the phase and Section 6.7 discusses the reliability and validity for Phase One's outcomes, and the chapter concludes in Section 6.8.

6.2 Phase One: Annotated bibliography

Evidence supports the existence of a security domain data corpus embodied within security textbooks that can be drawn on to explore explicit knowledge elements for the cultural domain of physical security (Chapter 5). The knowledge corpus for this phase

of the study stemmed from a literature critique of security texts utilizing a count analysis technique. Texts were selected due to their salient focus towards the domain practice area of physical security, primary crime prevention or security risk mitigation emphasis. Initial texts across the data corpus, texts 1 through to 9, discuss physical security and the associated knowledge requisites including technical knowledge underpinning physical protection systems (PPS) representing Stage 1 of the bibliographic extraction. Other texts consider security's non-traditional broader domain practice areas with groundings in criminology, engineering and management sciences. These texts, 10 – 15, represent Stage 2 of the data extraction.

Combined these texts formed an initial knowledge system (Table 6.16) based on extracted knowledge concept categories and supporting knowledge units (subordinate knowledge). These concept categories included concepts, theories, principles and fact elements selected according to the text's author's thesis or central claim, the repetition of key terms or ideas and the texts message and structure.

Included in the literature critique were prescribed texts from the ASIS requisite knowledge base, along with the International Foundation for Protection Officers (IFPO) course text, as knowledge priori. Such selection sought to ensure holistic capture of requisite knowledge areas for the non-traditional practice domain of physical security including technical, physical and procedural elements.

Consistent with Eden's (1988, p. 2) work, (Sections 1.8 & 4.2.1) extracted data from the selected texts provided repeated themes representing core and supporting knowledge requisites for physical security professionals as means of exploring a dispersed yet explicit knowledge base for physical security. For each text, the contents pages and chapter text (Section 3.3.1) were used to find repeated themes through key words (Kumar, 1996, p. 30) highlighting its salient superordinate and subordinate knowledge concept categories, content and units as they relate to theories, facts, principles and concepts as core and supporting knowledge subject areas of physical security. These were then assigned values accordant with occurrences within the text (Section 3.3.1**)** and in each text synonymous terms were combined (Manunta, 1999; Brooks & Corkill, 2012) (Appendix H) and the count of occurrences conducted again.

In addition, some frequently occurring words were dropped from the analysis. For example, international as a category word was removed, part was also removed as a category term, as was time. The word function was also removed during the analysis occurrences, as was physical. Furthermore, the category of management was removed from the word analysis due to jurisdictional conflict. For each text this produced a tabulated matrix highlighting its salient physical security knowledge concept categories. Each individual text's bibliographic extractions provided the initial knowledge category inputs towards establishing a phase knowledge matrix as a shared paradigm for physical security professionals.

6.3 Phase One: Bibliographic data extractions

6.3.1 Stage 1: Bibliographic extraction

Text 1: Garcia, M. L., (2008). The design and evaluation of physical protection systems (2nd ed.). Boston: Butterworth-Heinemann.

The first security text forming part of the data corpus is a textbook written by Mary Lynn Garcia from Sandia National Laboratories, Albuquerque, NM, USA. Garcia's biography explains that she is a Senior Member of the Technical Staff at Sandia National Labs. She has over 20 years' experience in science and engineering research, development, application, teaching, and project management of security systems and technology. Ms Garcia has been a Certified Protection Professional (CPP) since 1997. In addition, Ms. Garcia is the sole author of two texts within the security domain. Her first book The Design and Evaluation of Physical Protection Systems, first published in 2001, is now in its second edition (2008). Her second book, The Vulnerability Assessment of Physical Protection Systems was published in 2006. Ms Garcia's books have become embedded into many security teaching programs globally and her first book is listed as a core text for ASIS' Certified Protection Professional (CPP) program.

The Design and Evaluation of Physical Protection Systems (2nd ed.) articulates that the basic principles of security are the same regardless of application and that it is their adaption to context that is of salient importance. Such a statement is supportive of the body of knowledge concept. This text strongly emphasizes a systematic approach to security within a problem solving paradigm through the articulation of a Physical

Protection System (PPS), which combines technical, physical and procedural elements into a barrier system to achieve contextual protection objectives. Its salient purpose is to describe how individual elements that collectively make up an effective security system achieve this through their integration (Garcia, 2008, p. xvii). This includes defining and understanding the protection problem, accordant with conceptions of risk, prior to designing the treatment system. The text also emphasizes the importance of evaluating the design before and after implementation, along with ongoing review. On the basis of a count analysis, using key terms representative of synonymous words where necessary, Table 6.1 was developed as the knowledge concept categories for the reviewed text.

Table 6.1 Thematic knowledge category data: The design and evaluation of physical protection systems

Physical Security						
System	Sensors	Detection	Protection	CCTV	Alarm	Adversary
Design	Facility	Response	Security	Access	Assessment	Force
People	Delay	Threat	Information	Control	PPS	Intrusion
Communication	Doors	Analysis	Entry	Target	Assets	Lighting
Barriers	Data	Attack	Fields	Signal	Devices	Guard
Measurement	Equipment	Probability	Identification	Risk	Technology	Fences
Display	Functions	Zones	Nuisance	Computers	Level	EASI

Text 2: Walsh, T. J., Healy, R. J., Williams, T. L., Aggleton, D. G., Moritz, M. E., Hodge, M., Sherizon, S., Knoke, M. E., & Garcia, M. L. (2012). Protection of assets: Physical security. United States of America. ASIS International.

The next text in the physical security data corpus was ASIS International's Protection of assets: Physical security. ASIS International is a prominent, specialized society for security professionals, originally founded in 1955 as the American Society for Industrial Security. The Protection of assets series has been in existence since 1974, and is broadly recognized as a primary reference source for security professionals. The intention of the Protection of assets is to locate current, accurate and practical security treatment options across the broad range of asset protection subjects, strategies and solutions in a single reference source.

The text emphasizes the growing size and frequency of all forms of asset losses, coupled with the related increasing cost and complexity of countermeasures selection, and demands a systematic and unified presentation of protection doctrine across all

relevant practice areas (Walsh, et al, 2012). The Protection of assets sought to draw upon a large qualified source base to discuss salient elements of physical security in the protection of assets. On the basis of a count analysis, using key terms representative of synonymous words where necessary, Table 6.2 was developed as the knowledge concept categories for the reviewed text.

Table 6.2 Thematic knowledge category data: Protection of assets: physical security

Physical Security						
System	Security	Design	Facility	Protection	CCTV	Sensors
Alarms	Assets	Access	Detection	Lighting	Equipment	PPS
Control	Response	Assessment	Analysis	Information	Locks	Threat
Performance	Delay	Maintenance	Doors	Cost	Building	Crime
Risk	Adversary	Barriers	Personnel	Image	Devices	Lens
Contractor	Technology	Process	Procedures	Testing	Power	Assets
Digital	Surveillance	Fire	CPTED	Exterior	Construction	Standards

Text 3: Fennelly, L. J. (2013). Effective physical security (4th ed.). Boston: Butterworth-Heinemann.

The third reviewed text was written by Larry Fennelly who is a retired Director of Security for a Harvard Museum and former Harvard University Police Department Officer with more than 40 years' experience in the security domain. He attended the National Crime Prevention Institute at the University of Louisville, Kentucky and has been extensively involved with ASIS International. To date, he has written or edited 29 books collectively and is a well-known author and internationally accepted knowledge source within the security industry (crime prevention domain). Fennelly conveys that the book contains his combined knowledge and experience from his professional years. According to Fennelly, each chapter includes the current necessary specifics to ensure that practitioners can reference this text with a particular and immediate dilemma and come up with a practical amount of knowledge to help solve the moment's crisis.

The book is divided into discrete yet interwoven themes emphasizing influences in the design of physical security including strategies, along with individual knowledge areas. These areas include physical barrier considerations and building fabric, the use of technology to provide surveillance and control access, and fire life safety. These are supported by an introduction into standards and regulations in the American context and

security officers and equipment considerations. The theme of the text is about controlling physical access to ensure that only authorized persons gain access to a facility and property. On the basis of a count analysis, using key terms representative of synonymous words where necessary, Table 6.3 was developed as the knowledge concept categories for the reviewed text.

Table 6.3 Thematic knowledge category data: Effective physical security

Physical Security						
Security	System	CCTV	Doors	Locks	Access	Alarms
Keys	Protection	Lighting	Control	Data	Design	Devices
Bolts	Fences	Building	Windows	Sensor	Fire	Risk
Crime	Facility	Pin	Barriers	Safes	Combinations	Network
Attack	Cylinder	Standards	Glass	Images	Lens	Tumbler
Signal	Threat	Line	Scene	Assessment	Personnel	Interior
Costs	Digital	Process	Badges	Guards	Exterior	Electrical

Text 4: Baker, P. R., & Benny, D. J. (2013). The complete guide to physical security. Boca Raton, FL. CRC Press.

The next reviewed text was co-written by Paul Baker and Daniel Benny. Paul Baker holds a Bachelor of Science in Administration of Justice, a Masters of Business Administration, a Master's of Science in criminal justice and a Doctorate of Strategic Leadership and is Certified Protection Professional (CPP). His employment history includes the United States Marine Corps, Maryland Police Department, the MITRE Corporation, Institute for Defence Analysis and the RAND Corporation. Dr Baker is an adjunct professor for the University of Maryland University College in the homeland security field and an adjunct professor for Southwestern College in its security management curriculum.

Daniel Benny holds a Bachelor of Arts in Security Administration, Associate in Arts in both Commercial Security and Police Administration, a Master of Arts in Security Administration, Master of Aeronautical Science and a Doctor of Philosophy (PhD) in criminal justice. He is the security discipline chair at Embry-Riddle Aeronautical University. Dr Daniel Benny has authored books including General aviation security: aircraft, hangars, fixed base operations, flight schools; and Airports and cultural

property security: protecting museums, historic sites, archives, and libraries; as well as over 3oo articles on security administration, intelligence, aviation security, private investigation, and cultural property security topics. His professional career includes service as a US Naval intelligence officer, Central Intelligence Agency employee, Director of Protective Service Pennsylvania Historic and Museum Commission, and as a US Navy police chief.

The text both recognizes and emphasizes the need to train the newly recruited members of the physical security trade and make them aware of the nuances of this occupational field. The text premises that the knowledge base for the field of physical security which pulls into place access control, closed-circuit television, intrusion detection and environmental controls is partly technical and partly physical. In addition, the text expresses that decisions concerning the application of the physical security body of knowledge cannot be made in a vacuum, they are made cognizant of the business context for which the controls are facilitating the achievement of objectives. Therefore the text states that it will address each topic from the standpoint of common-sense in relation to business dynamics and security leadership. On the basis of a count analysis, using key terms representative of synonymous words where necessary, Table 6.4 was developed as the knowledge concept categories for the reviewed text.

Table 6.4 Thematic knowledge category data: The complete guide to physical security

Physical Security						
Security	System	Protection	CCTV	Control	Access	Leadership
Facility	Building	Design	Guards	Costs	Doors	Organization
Biometric	Locks	Alarms	Devices	Surveillance	Entry	Lighting
Technology	Information	People	Identify	Planning	Fire	Keys
Business	Threat	Level	User	Sensors	Detection	Force
Images	Application	Card	Risk	Visitor	Network	Procedures
Assessment	Intrusion	Project	Process	Emergency	Monitoring	Response

Text 5: Garcia, M. L. (2006). The vulnerability assessment of physical protection systems. Boston: Butterworth-Heinemann

The next security text forming part of the data corpus is another textbook written by Mary Lynn Garcia from Sandia National Laboratories, Albuquerque, NM, USA who also authored the first text reviewed. Text 5 describes the entire vulnerability assessment process for a physical site from the start of the planning through to final analysis and then briefing components to senior management. The text is described as an extension of The design and evaluation of physical protection systems (Text 1). The underlying premise of this text is that overall system effectiveness is the prime objective for a physical security system, also referred to as a physical protection system (PPS). Mary Lynn expresses that the goal was to write a thorough, but not overly detailed, description of the common vulnerabilities of physical protection systems. The text is divided into discrete chapters with chapter one providing an overview of risk management, vulnerability assessment and systems engineering principles. The following chapters describe the PPS and articulate how to assess for adversary vulnerabilities. On the basis of a count analysis, using key terms representative of synonymous words where necessary, Table 6.5 was developed as the knowledge concept categories for the reviewed text.

Table 6.5 Thematic knowledge category data: The vulnerability assessment of physical protection systems

Physical Security						
Sensors	System	Alarms	CCTV	Response	Assessment	Detection
Facility	Personnel	Analysis	Subsystem	Delay	Adversary	Control
Project	Security	Protection	Assets	Attack	Evaluation	PPS
Data	Information	Doors	Threat	Entry	Testing	Personnel
Intrusion	Report	Fences	Barriers	Communication	Functions	Design
Display	Equipment	Vehicle	Installation	Maintenance	Materials	Components
Signal	Access	Lighting	Exterior	Probability	Portal	Vulnerability

Text 6: Khairallah, M. (2006). Physical security systems handbook: The design and implementation of electronic security systems. Burlington, MA: Butterworth-Heinemann.

The next text in the reviewed data corpus is one written by Michael Khairallah. Khairallah premises that the text is written as a comprehensive guide to identifying the human-centred threats to an organization, determining the vulnerabilities of the organization to those threats, specifying security products to mitigate said threats and acquiring and implementing the recommended solutions.

Khairallah states that the depth of detail in the book assumes the reader is a security professional and has both experience and the technical skills necessary to create a basic security system design. The main emphasis of the text is to provide the security professional with a guide for doing the right things at the right time throughout all phases of a physical security process. The text is divided into discrete chapters including threat assessment, and vulnerability analysis, preliminary system design, presenting solutions and system acquisition and implementation. On the basis of a count analysis, using key terms representative of synonymous words where necessary, Table 6.6 was developed as the knowledge concept categories for the reviewed text.

Table 6.6 Thematic knowledge category data: Physical security systems handbook: The design and implementation of electronic security systems

Physical Security						
System	Security	Doors	Vendor	Control	Access	Installation
Bid	Devices	Equipment	CCTV	Cards	Alarm	Lock
Costs	Design	Threat	Planning	Project	Opening	Recommendations
Electrical	Employees	Requirements	Identify	Process	Meeting	Cable
Protection	Facility	Power	Perimeter	Assets	Drawings	Response
Information	Monitoring	Assessment	Reports	Vulnerability	Acceptance	Review
Testing	Document	Reader	Evaluation	Data	Level	Lighting

Text 7: Pearson, R. L. (2007). Electronic security systems: A manager's guide to evaluating and selecting system solutions. Burlington, MA: Butterworth-Heinemann.

This text is focused towards imparting the knowledge required for implementing and managing technical security components as a holistic system. The author notes that while the technical sophistication of security systems has increased, many security professional's knowledge of these aspects has not kept pace. Pearson highlights that in the early days the physical security profession focused on the physical aspects of security as the available electronic systems possessed only very rudimentary capabilities. However, now broader system philosophies and technical understandings are required, especially in terms of how individual technologies operate with other system elements to achieve system objectives.

The focus of this text is therefore to enable the security professional understand the various electronic security functional components and the ways these components interconnect, as well as provide a guide to a holistic approach to solving security issues with various technologies. The text discusses issues of integrating electronic security functions, developing a system, component philosophy, long-term system issues, and the culture within a corporation which will impact the final system design. The author premises that electronic solutions are as much an art form as a science, stating "there is not just one solution to a given problem". On the basis of a count analysis, using key terms representative of synonymous words where necessary, Table 6.7 was developed as the knowledge concept categories for the reviewed text.

Table 6.7 Thematic knowledge category data: Electronic security systems: A manager's guide to evaluating and selecting system solutions

Physical Security						
Security	System	Alarms	Badges	Electrical	Control	Access
CCTV	Fields	Panel	Cables	Data	Sensors	Technology
Fire	Database	Doors	Devices	Costs	Detectors	Operator
Installation	Functions	Level	Software	Building	Employees	Standards
Maintenance	Design	Computer	Applications	Project	Integration	Reader
Lighting	Automation	Information	Location	Server	Facility	Protection
Code	Biometric	Testing	Wireless	Communication	Power	Monitoring

Text 8: Norman, T. L. (2007). Integrated security systems design: Concepts, specifications and implementation. Burlington, MA: Butterworth-Heinemann.

This text is about designing convergence-based integrated security systems and enterprise integrated security systems. Technological advances have seen both components and functions in the security management plan integrated to achieve a desired level of security. The text premises that many in the security domain fail to comprehend the technological advances and requirements of contemporary ethernet infrastructure security systems. Norman states that since 2003 the security industry left behind the 'old technology', now security technology is information technology (IT) based, and many in the security industry are afraid of it. Therefore this text is written for new and experienced system design consultants, designers, and project managers who build these complex systems and for building owners, security directors and facilities directors who operate them. On the basis of a count analysis, using key terms representative of synonymous words where necessary, Table 6.8 was developed as the knowledge concept categories for the reviewed text.

Table 6.8 Thematic knowledge category data: Integrated security systems design: Concepts, specifications and implementation

Physical Security						
System	Security	CCTV	Doors	Design	Control	Access
Alarms	Networks	Devices	Switching	Digital	Locks	Data
Interface	Cards	Building	Guards	Project	Electrical	Server
Detectors	Technology	Intercom	Console	Power	Signal	Communication
Monitoring	Reader	Functions	Software	Fire	Detection	Hardware
Configuration	Code	Transmission	Contractor	Information	Field	Drawings
Integrated	Barriers	Environment	Electrified	Antenna	Specifications	Infrastructure

Text 9: Contos, B. T., Crowell, W. P., DeRodeff, C., Dunkel, D, & Cole, E. (2007). Physical and logical security convergence: Powered by enterprise security management. Burlington, MA: Syngress.

Brian Contos holds a Bachelor of Science and is currently in the position of Chief Security Officer, ArcSight Inc. In this role he advises government organizations and Global 1, 000 Companies on security strategy related to Enterprise Security Management (ESM) solutions. Dan Dunkel is an information technology (IT) sales executive and operates his own consultancy firm, New Era Associates; a private consultancy specializing in sales strategy and business partner development between IT and physical security vendors and integrators. He is a frequent speaker at security trade shows in the United States and writes a twice monthly column for Today's Systems Integrators, (TSI), an online publication of Security Management and BNP Publishing.

William Crowell is an independent consultant specializing in information technology, security and intelligence systems. An expert on network security issues, Crowell served as President and Chief Executive Officer of Santa Clara and then California-based Cylink Corporation a leading provider of e-business security solutions after a substantial period with the National Security Agency (NSA). Since 9/11 he has served on Markle Foundation Task Force on National Security in the Information Age. Colby DeRodeff is the manager of Technical Marketing at ArcSight. His expertise is focused towards the insider threat and the convergence of physical and logical security, as well as enterprise security and information management.

Eric Cole currently works in research and development to advance the state of the art in information systems security. He holds a Masters in Computer Science and a PhD with a concentration in Information Security. He has authored a number of books including Hackers beware, Hiding in plain sight, as well as Insider threat. He is an inventor with over 20 patents to his name along with being a researcher, writer and speaker for the SANS Technology Institute.

The text premises that the convergence between physical and cyber security affects contemporary security solutions. This is a single source text aimed at linking the two traditional domain knowledge bases of physical and cyber security stressing that

corporate security must understand and implement converged security or be left vulnerable. As such, the text is marketed towards anyone who wishes to be a leader in the security field, IT or physical security as the text takes an in-depth look at how the issue of convergence is impacting enterprise security, particularly from the insider threat perspective. On the basis of a count analysis, using key terms representative of synonymous words where necessary, Table 6.9 was developed as the knowledge concept categories for the reviewed text.

Table 6.9 Thematic knowledge category data: Physical and logical security convergence: Powered by enterprise security management

Physical Security						
Security	System	Networks	Log	Technology	Access	Information
Data	Syngress	Control	CCTV	Process	Attack	Analysis
User	Protection	Devices	Critical	Policy	Infrastructure	Deployed
Threats	Assets	Server	Standards	Communication	Detection	Integration
Model	Response	Internet	Logical	Identity	Monitoring	Leadership
Level	Sensors	Environment	Vendors	Surveillance	Analyst	Applications
Intelligence	Computers	Governance	People	Software	Trusted	Source

6.3.2 Stage 2: Bibliographic extraction

Text 10: Broder, J., & Tucker, E. (2012). Risk analysis and the security survey (4th ed.). Waltham, MA: Butterworth-Heinemann.

The analysis of this work represents the commencement of stage two of the literature extraction in which texts based security's non-traditional broader-domain practice areas are reviewed.

This text was written for security and risk management professionals and is the fourth edition of the original text published in 1984. It provides an understanding of the principles of risk analysis for security students and professionals including the two elements of risk control: (1) the protection of assets by identifying, analysing, and prioritizing the risk, and (2) contingency and disaster recovery planning. The authors state that "when security fails, as it occasional does, recovery becomes paramount and security professionals must understand the vital role they play if they are to fully meet their responsibilities".

James Broder is a former Federal Bureau of Investigation (FBI) special agent and US State Department employee. Combined he has more than forty years' experience in security and law enforcement, having worked as a security executive, instructor and consultant. Eugene Tucker is the head of Praetorian Protective Service and a past member of the board of directors for the Business recovery Managers association in the United States. On the basis of a count analysis, using key terms representative of synonymous words where necessary, Table 6.10 was developed as the knowledge concept categories for the reviewed text.

Table 6.10 Thematic knowledge category data: Risk analysis and the security survey

Security						
Security	Risk	System	Survey	Analysis	Recovery	Response
Employees	Control	Planning	Emergency	Identify	Report	Loss
Organization	Information	Hazards	Continuity	Fire	Data	Costs
Building	Equipment	Incident	Protection	Crime	Threat	Damage
Disaster	Facility	Procedures	Preparedness	Prevention	Impact	Operations
Plans	Consultant	Method	Strategies	Standards	Crisis	Materials
Safety	Level	Training	Policy	Testing	Flood	Evacuation

Text 11: International Foundation for Protection Officers (IFPO) (2012). The professional protection officer: Practical security strategies and emerging trends (8th ed.). Burlington, MA: Butterworth-Heinemann.

The International Foundation for Protection Officers (IFPO) is a not for profit organisation established in 1988, headquartered in Tampa, Florida in the United States. As an organisation it seeks to provide education and certification to protection and security officers in the United States of America, Canada, and throughout the world, develop and maintain security training standards that improve the quality of job performance of protection and security officers, establish standards of ethics for protection and security officers and to encourage adherence to these standards and also fund research projects that will further educational opportunities for protection and security officers.

The purpose of this text is to provide what the International Foundation for Protection Officers (IFPO) consider are the 'need-to-knows' or knowledge requisites for protection officers and students throughout the security industry and is a course text for the

Certified Protection Officer program (CPO) through the International Foundation for Protection Officers (IFPO). The book is premised on the view that the principles of security always apply though the contexts differ, but that those principles need to be adapted to meet local needs. Therefore this text serves as a research resource for those looking to develop insight into an array of security topics. On the basis of a count analysis, using key terms representative of synonymous words where necessary, Table 6.11 was developed as the knowledge concept categories for the reviewed text.

Table 6.11 Thematic knowledge category data: The professional protection officer: Practical security strategies and emerging trends

Physical Security						
Security	Officer	Protection	Crime	People	Control	System
Risk	Law	Information	Employees	Organization	Training	Safety
Alarms	Threat	Assets	Access	Incident	Response	Force
Communication	Prevention	Work	Hazards	Emergency	Services	Detection
Patrol	Personnel	Terrorism	Violence	Facility	Loss	Level
Property	Costs	Drug	Equipment	Report	Planning	Identify
Technology	Theft	Keys	Crowd	Procedures	Weapons	CCTV

Text 12: Fischer, R. J., Halibozek, E., & Green, G. (2008). Introduction to security (8th ed.). Boston: Butterworth-Heinemann.

The next text in the security data corpus is a textbook co-written by three authors within the security domain. Robert Fischer whose biography highlights that he is a member of the Academy of Criminal Justice Sciences, and holds a PhD. He is currently President of Asset Protection Associates, Inc, a security consulting company. Robert Fischer is a former Director of Illinois Law Enforcement Executive Institute and a Professor of Law Enforcement and Justice Administration at Western Illinois University. Edward Halibozek is the former Chairperson for the Aerospace Industries Association, Industrial Security Committee and is currently a member of the Board of director for the Chief Special Agents Association in Los Angeles in addition to being a corporate director of security for a fortune 100 Company. Gion Green is noted in the book to be a twentieth century security pioneer.

Together these professionals wrote Introduction to security (8th ed.). This text forms part of the ASIS international knowledge corpus and sought to establish for the reader the basic concepts of security. In addition, the text introduces learners to the depth and breadth of the security domain in the non-traditional sense. Furthermore, the text has sought to articulate the current problems within the basic frameworks of security theory in response to the changing global posture in a post September 11th, 2001 environment. Especially in the areas of terrorism; this included a new emphasis also focusing towards securing information, identity theft, transportation, contingency planning and piracy concerns.

The text aims to introduce security concepts and approaches to those new to the industry along with serving as a reference text for professional problem solving within the security domain. This text is divided into three sections; Section one presents the security domain, history, employment options and professional development. Section two presents the basics of defence and Section three focuses towards specific threats and solutions within security context areas. Of significance for this study is that the text (p. 173) highlights that while every security program must be an integrated whole, and that individual elements must grow out of the needs dictated by the circumstances, the first basic line of defence is still physical security (Section 2). That is, the physical protection of the facility through the meticulous attention to detail. On the basis of a count analysis, using key terms representative of synonymous words where necessary, Table 6.12 was developed as the knowledge concept categories for the reviewed text.

Table 6.12 Thematic knowledge category data: Introduction to security

Physical Security						
Security	People	System	Terrorism	Protection	Law	Crime
Control	Information	Computer	Loss	Reports	Theft	Facility
Planning	Alarms	Prevention	Locks	Costs	Building	Training
Drug	Risk	Response	Access	Devices	Doors	Work
Threat	Safety	Keys	Emergency	Violence	Property	Policy
Standards	Force	Attack	Cards	Level	Lighting	Data
Technology	Surveys	Procedures	Internal	Design	Equipment	Contract

Text 13: Smith, C., L. & Brooks, D., J. (2013). Security science: The theory and practice of security. Waltham, MA: Butterworth-Heinemann.

The next text in the reviewed data corpus is a text which emphasises the multi-disciplined practice areas of security into a single structured body of knowledge. Clifton Smith is a physicist and currently an honorary professor with Edith Cowan University (ECU) in Western Australia. Clifton Smith initiated the establishment of the Australian Institute of Security and Applied Technology at ECU in 1987, and developed research profiles in in security imaging, biometric imaging, ballistics identification, and infrared sensing. He also developed the first Bachelor of Science (security) honours degree, a Masters' of Science (Security science) research degree, and doctor of philosophy (Security science) research degree. David Brooks (PhD) has over 33 years' experience in the security domain with the U.K. Royal Air Force, Australian Department of Defence, as a professional consultant and security educator. David maintains a role as a security research leader within Edith Cowan University's Security Research Institute (SRI).

Within this text each chapter takes an evidence-based approach to one of the core knowledge categories. Unlike many security texts the authors provide the underlying scientific basis supporting underlying theories, principles, models or frameworks within the domain of security. Demonstrating the relationships and underlying concepts, they present an approach to each core security function within the context of both a national and organizational security perspective. The text provides a rational basis for complex decisions and begins the process of defining the emerging discipline of security science. On the basis of a count analysis, using key terms representative of synonymous words where necessary, Table 6.13 was developed as the knowledge concept categories for the reviewed text.

Table 6.13 Thematic knowledge category data: Security science: The theory and practice of security

Physical Security						
Security	Risk	System	Organization	Planning	Data	Detection
Process	Technology	People	Facility	Threat	Assets	Environment
Control	Protection	Barriers	Intelligence	Assessment	Access	Strategy
Response	Application	Design	Critical	Biometric	Concepts	Devices
Testing	Fire	Attack	Functions	Analysis	Crisis	Standards
Decisions	Science	Equipment	Principles	Context	Safety	Theory
Identification	Integrated	Costs	Resources	Intruder	Probability	Evaluation

Text 14: Atlas, R. (2013). 21st Century security and crime prevention: Designing for critical infrastructure protection and crime prevention (2nd ed). Taylor & Francis. Boca Raton, FL.

Randall Atlas is an architect and criminologist. He is president of Counter Terror Design Inc; and vice president of Atlas Safety & Security Design, holding a Bachelor's Degree in Architecture and Criminal Justice, a Master's Degree in Architecture, and a Doctorate in Criminology. Randall Atlas is a nationally recognized speaker in the United States and has worked professionally for the National Crime Prevention Institute, the American Institute of Architects, and the American Society of Industrial Security (ASIS). He is a Certified Protection Professional (CPP) with ASIS and a member of the Security Architecture and Engineering Council. Randall also serves on the American Society of Testing Materials (ASTM), f33 Committee on Corrections and Detention Facilities, and the ES4 Committee on Homeland Security. In addition, Atlas has contributed to the Protection of assets manual and written for security interest magazines including: Access Control & Security Systems, Security Technology & Design, and Security Management.

The text discusses the competing needs framed by the American culture of openness and access versus the need for protection from threats to security and safety. Atlas acknowledges that many architects do not recognize the requisite to design security into the built environment because it does not relate to them. Premising that many architects have never studied security approaches such as crime prevention through environmental

design (CPTED) in their educational courses. Atlas expresses the need for balanced security, stating that the real issue is what level of inconvenience will be tolerated by the imposition of security before people just avoid the activity or space. On the basis of a count analysis, using key terms representative of synonymous words where necessary, Table 6.14 was developed as the knowledge concept categories for the reviewed text.

Table 6.14 Thematic knowledge category data: 21st century security and crime prevention: Designing for critical infrastructure protection and crime prevention

Physical Security						
Security	Building	Lighting	Design	CPTED	Access	Crime
Facility	System	People	Control	Risk	Design	Level
Environment	Community	Threat	Prevention	Surveillance	Natural	Doors
Safes	Standards	CCTV	Assets	Property	Assessment	Safety
Windows	Architectural	Criminal	Landscaping	Codes	Infrastructure	Fences
Exterior	Critical	Costs	Terrorism	Vulnerability	Glass	Zones
Employees	Alarms	Planning	Walls	Emergency	Information	Energy

Text 15: Fennelly, L. (2012). Handbook of loss prevention and crime prevention (5th ed.). Butterworth-Heinemann. Waltham, MA.

The final text in the data corpus is a security textbook written by Larry Fennelly who also wrote Text 3. Fennelly considers that crime is a fact of life and that security is a process which must be part of the ongoing business practice. The text is premised to assist the security professional determine the goal of the security process, to control access, to protect assets and inventory, to prevent robberies and burglaries, to monitor life safety systems, to reduce potential liability, to reduce insurance premiums and to ensure business continuity. He expresses the view that there are layers in every security program designed to protect people, buildings and property and that the more valuable or vulnerable the subject being protected the more layers required in the security process. The text focuses towards traditional security element topics as they help achieve security layers including access control, security barriers, risk management and the dynamic security environment. This text has been written towards what Lawrence Fennelly believes today's security practitioner needs to practice. On the basis of a count analysis, using key terms representative of synonymous words where necessary, Table 6.15 was developed as the knowledge concept categories for the reviewed text.

Table 6.15 Thematic knowledge category data: Handbook of loss prevention and crime prevention

Physical Security						
Security	People	System	Protection	Locks	Crime	CCTV
Doors	Control	Building	Keys	Procedures	Facility	Information
Design	Planning	Alarms	Access	Lighting	Risk	Threats
Reports	Emergency	Devices	Data	Identification	Fire	Response
Attack	Theft	Property	Level	Cards	Safety	Loss
Bolts	Assets	Detection	Fences	Standards	Combination	Guards
Cylinder	Vehicles	Analysis	Network	Entry	Interior	Barriers

6.4 Phase One: Findings

Consistent with the theoretical framework set forth in Section 1.8, Phase One of the study sought to understand the explicit knowledge domain of physical security as expressed by repeated themes (constructs or concepts) as depicted across a selection of relevant security texts.

Phase One sought to respond to the question: *What are the explicit knowledge concept categories for physical security as represented through repeated themes printed in security texts and their structure*?

Repeated themes were extracted using a word count analysis accordant with the work of Kumar (1996) (Section 4.2.2), and then sorted according to frequency count from highest to lowest. As Kumar (1996, p. 26) expressed, the print (published) domain represents a large trove of data. In addition, the work of Guest, MacQueen and Namey (2012, p. 6) explained that a mathematical analysis of word occurrence from such texts is a legitimate form of analysis (See Section 4.2.2).

Accordant with the frequency count across the sampled texts, salient knowledge categories and concepts emerged which were tabulated into a final seven by seven matrix from highest to lowest occurrence representing the top 49 knowledge categories, concepts and principles to develop Phase One's bibliographic knowledge concept categories (Table 6.16). Consistent with Kumar's (1996, p. 30) work, Table 6.16 is organized according to their summated occurrence from highest to lowest as an interim cultural taxonomy.

Table 6.16 Phase One: Data corpus thematic knowledge categories

Physical Security						
Security	System	CCTV	People	Control	Access	Design
Alarms	Facility	Doors	Crime	Building	Risk	Information
Lighting	Threat	Sensors	Detection	Response	Data	Locks
Assets	Planning	Device	Lenses	Analysis	Technology	Assessment
Emergency	Costs	Attack	Standards	Keys	Report	Safety
Equipment	Fire	CPTED	Network	Barriers	Procedures	Fencing
Prevention	Loss	Adversary	Property	Terrorism	Guard	Law

Table 6.16 highlights that the most frequently occurring theme from the data extraction was the word security. That is, the very concept of security overarched all others. Such an outcome is congruent with the work of Spradley (1979) (Section 1.5) who expressed the view that a cultural domain's knowledge structure is based on isolating the fundamental units of cultural knowledge accordant with a single semantic relationship with their cover term. For this study the cover term was premised, and subsequently found to be, the term security (Section 2.2). Following the concept of security were 48 additional fundamental units of cultural knowledge represented through their knowledge concept category cover terms. Each of the knowledge concept categories within the cultural table (Table 6.16) represents a cover term for an area of relevant domain knowledge with its own body of literature, which is essential for professional practice within the occupational domain of physical security.

The knowledge concept category table (Table 6.16) is supported by a word cloud (Figure 6.1) developed using Nvivo software based on all texts from the data corpus using the top 100 results from the word frequency query. Word clouds provide a visual representation of frequently occurring themes or concepts across analysed texts where font size and colour intensity increases proportionally based on the weighted percentage of each item extracted. The most salient term is placed at the centre of the cloud, at the largest font size and brightest colour, and subsequent terms are placed in sequence around this using a font size, location and colour intensity determined by their weighted percentage.

The word cloud developed for this study supports that the word security is the most salient concept within the data corpus, closely followed by system and systems. Also

appearing as salient concepts are control, access and protection. Then concepts such as risk, alarm, design, physical and information follow, emphasizing their significance within the domain of physical security.

Figure 6.1 Nvivo word cloud of key words and concepts for the cultural domain of physical security.

Drawing on the writings of Maher and Burke (1991, p. 13), Kumar (1996, p. 30) and Bernard and Ryan (2010, p. 8) (Sections 4.2.1 & 4.2.2) Phase One used the outcomes of the pilot study as a new priori. Accordant with the principles of constructivism (Section 1.8), knowledge categories from the pilot study experts (Table 6.17) were bought forward for use in Phase One. These included 18 categories, not uncovered in the literature extraction, but articulated by participants in the pilot study as important knowledge areas for physical security professionals.

Table 6.17 Pilot study: Carried forward knowledge concept categories

Physical Security			
Door furniture	Defence in depth	Situational crime prevention	Infrastructure
Structural strengths	Safes & vaults	Electric power	Delay
Surveillance	Windows	Glass	Walls
Drugs	Interruption	Field of view	Security surveys
Movement control	Communication		

The combination of the Phase One literature extraction along with the concept categories brought forward from the pilot study provided inputs for an enhanced cultural domain knowledge concept category table (Table 6.18) and hierarchical knowledge concept category table (Table 6.19) accordant with the writings of Spradley (1979) (Section 4.2.3).

Table 6.18 Phase One: Physical security knowledge concept categories

Physical Security						
Security	System	CCTV	People	Control	Access control	Planning & design
Alarms	Facility contextualization	Doors	Crime	Building	Risk	Data & Information
Lighting	Threat	Sensors	Detection	Response	Locks	Assets
Device	Lenses	Analysis & evaluation	Technology	Emergency	Costs	Attack
Standards	Keys	Reports	Safety	Equipment	Fire	CPTED
Network	Barriers	Procedures	Fencing	Prevention	Loss	Adversary
Property	Terrorism	Guard	Law	Door furniture	Defence in depth	Situational crime prev
Infrastructure	Structural strengths	Safes & vaults	Electric power	Delay	Surveillance	Windows
Glass	Walls	Drugs	Interruption	Field of view	Security surveys	Security theory & principles
Movement control	Resolution					

The premise of the study was that Physical Security, as a sub-domain of non-traditional security, has its own knowledge base that can be formally codified. Such knowledge may stem from other domain disciplines including engineering, physics, architecture, criminology, law, psychology and sociology, along with other domains that can contribute to a fused knowledge system. Such domain knowledge can be fused to develop a single codified taxonomic framework (Table 6.19) accordant with the work of Eden (1988) (Section 1.8). Many domains are understood through taxonomic structure (Anderson & Sosniak, 1994, p. 11).

Eden's (1988, p. 2) work expressed that man seeks to make sense of his world through the detection of repeated themes and the construal of them using a construct system such as a taxonomy. Tables 6.18 and 6.19 along with Figure 6.2 represent such a taxonomic construct system. As Spradley (1979, p. 137) explains, taxonomies are subsets of domains; tangible sets of content classifications organized on the basis of a single semantic relationships which articulate the core knowledge and broader educational outcomes as a system reflective of that knowledge required to practice at a professional level.

Table 6.19 and Figure 6.2 support that the cultural domain of physical security is based on, and organized hierarchically from the word and overarching concept of security, as it appeared the most frequently in the summated word extraction of all texts. Table 6.19 and Figure 6.2 further highlight that the relations in a knowledge system can be revealed through the use of heuristics as useful tools for providing a conceptual net or template of order and structure to the domain (Krimsky and Golding, 1992, pp. 9-19) (Section 3.10) of physical security.

Table 6.19 Phase One: Hierarchical knowledge concept category table

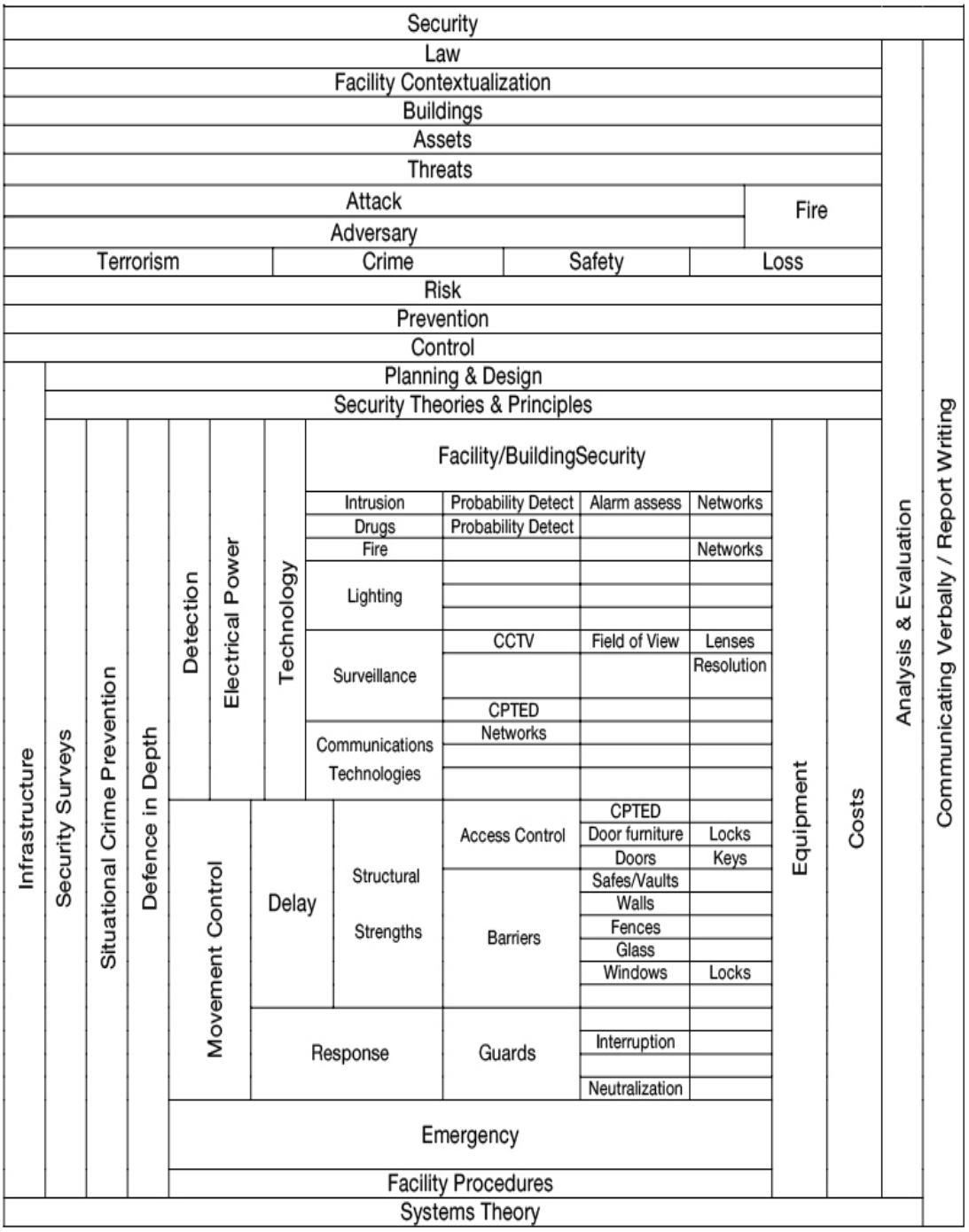
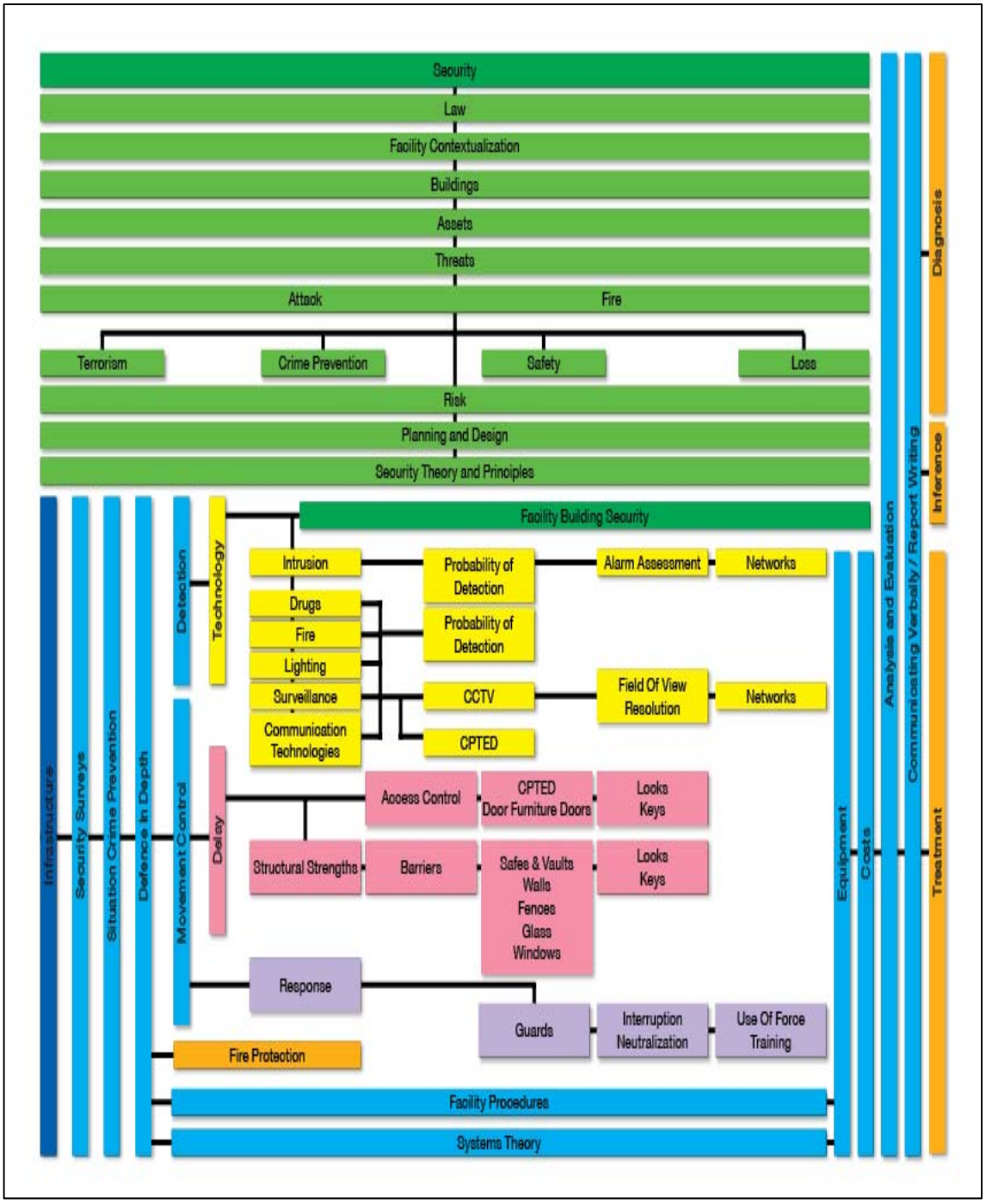


Figure 6.2 Phase One: Physical security knowledge structure heuristic



6.5 Phase One: Interpretation

The combined works of Horrocks (2001), Axt (2002) and Smith and Brooks (2013) (Section 1.6) highlight that for physical security to emerge as a profession, it must be based within a generalizable curriculum. Such a curriculum would, as a shared paradigm, explicitly state the various practice areas' knowledge content, its structural properties, and include interrelations. It would also demonstrate how it is supported by broader academic attributes essential for professional practice.

The current findings of the study suggest that Tables 6.18 and 6.19 along with Figure 6.2 present, as iterations, such a knowledge system. Table 6.18 provides a phase list of core and supporting knowledge concept categories as requisites for professionals to hold in their endeavours to treat society's security loss or risk concerns manifested through unlawful access or crime enablers in the protection of assets that includes people, information and property (Section 3.3).

Such knowledge is expressed by Abbott (1988) as abstract knowledge which culturally relates to the diagnosis, inference or reasoning about and treatment of particular problems based on domain specific concepts, principles and theories (1988, pp. 36-41). Fitting with the combined works of Kelly (1955), Bruner (1977), Eden (1988) Fraser (1993), McLucas (2003) and Fosnot (2005), Tables 6.18 and Table 6.19 collectively form a knowledge system or body of knowledge built on the academic disciplines on which the domain's content areas are constructed from. This knowledge can be organised in ways that enhance understanding for novice learners, facilitating the remembering of ideas, materials or phenomena. Such organisation also facilitates the integration of new knowledge into existing knowledge structures. Phase One of the study sought to respond to the question: What are the explicit knowledge concept categories for physical security represented as repeated themes printed in security texts and their structure?

Phase One of the study indicates that the published knowledge concept categories include those presented in Table 6.16. These were collated from Tables 6.1 through to 6.15 representing salient knowledge categories from each reviewed text and represent Phase One's data corpus of knowledge concept categories for physical security

professionals. However, these data were integrated with Table 6.17 which presented knowledge concept categories carried forward from the pilot study (Chapter 5). Accordant with the principles of constructivism, combining Tables 6.16 and 6.17 lead to the development of Table 6.18.

From this, through the analytical procedures of Spradley (1979), Johnson and Christensen (2004) and Bernard and Ryan (2010) (Section 4.2.3), Table 6.19 was developed depicting hierarchical relationships showing relations and connections revealing significant knowledge requisites. Table 6.19 led to the development of Figure 6.2 to produce an interim heuristic symbol for communicating concept categories and their relations forming a physical security body of knowledge as a shared paradigm (Section 1.8).

Bruner's (1977, p. 12) work highlighted that teaching and learning of structure, rather than simply mastery of facts and techniques is at the centre of enhanced knowledge transfer. Knowledge structure is especially important when explaining the relations between concepts encountered earlier and later when establishing new knowledge. Such structure can be presented taxonomically, for instance, Table 6.19 supports that knowledge structure for the domain of physical security can be represented through a taxonomy, organised based on a single semantic relationship with its cover term. Such taxonomies (Table 6.19) can be illumed through cognitive or conceptual maps (Posner & Rudnitsky, 1982, pp. 8-39) (Figure 6.2) as these are concerned with the relationships among ideas, based on organising them in some reasonable pattern or structure depicting relationships in both simple and complex terms. As with Figure 6.2 they can be organised hierarchically, or in some other way that forces the expression of broader themes.

In addition, Table 6.19 and Figure 6.2 support the propositions that knowledge is constructed not discovered (Section 1.8) and that it is built on the foundations of previous knowledge which may include printed domain knowledge or that offered by those working in the field. Furthermore, specific cultural knowledge is constructed from the detection of repeated themes (Tables 6.16, 6.17 and 6.18) organised hierarchically through contrast and similarity (Table 6.19) (Eden, 1988). These constructs indicate how physical security's literature base along with experts' knowledge can fit together.

For example, Figure 6.2 highlights that some knowledge is used to diagnose the security or crime problem, other knowledge is focused towards professional inference or reasoning about the problem. Then more technical knowledge is focused towards treating the problem, and all this is supported by professional enabling attributes.

Eden's (1988, p. 8) work expressed that man seeks to develop meaningful patterns of constructs of his world. Tables 6.18 and 6.19 along with Figure 6.2 provide another iteration of a literature centred, expert enriched construct of meaningful patterns representing physical security's knowledge base. From an educational standpoint, consistent with the works of Ausubel (1968) and Novak (1993) (Section 1.8) they are also useful tools for drawing out expert understanding of their world and building on the knowledge system through their lived experience. Phase One findings will be used to provide the means for security professionals working in the field to visualise the concepts and interim structure and add to this explicit knowledge system their implicit knowledge accordant with their lived experiences within the domain of physical security.

6.6 Phase limitations

This phase of the study experienced a number of research limitations that influenced the findings. These include:

- Variations in security language, or rather variations in how terms are used to express meaning. Security does not have a domain discipline dictionary of agreed terms. Language variations in the security domain have been recognized by Manunta (1999) and these cannot be ignored as potential comprehension biases in forming knowledge categories from the literature extraction;
- The synergy of synonymous terms also represented a potential limitation within the study. While the study attempted to address variations in language and category meanings, the interpretations and selection of language represented a snapshot of the reviewed literature and expert participant's views rather than a consensus across the broader security domain; and
- The selection of texts was another limitation within the study. A data corpus of 15 books provided a small snapshot of available security texts, presenting sources

limitation. Nevertheless, the selection of salient texts for physical and the broader non-traditional security domain including those from the ASIS knowledge base sought to minimize this limitation.

6.7 Reliability and validity

Textual data are, in principle, reliable sources for analysis (Silverman, 2002, p. 229). In addition, to enhance validity of the count analysis, the software program Nvivo was used providing objective categories external from the researcher. The use of software tools for qualitative analysis is supported in the writings of Liamputtong and Ezzy (2006, p. 274). In addition, the data extraction and knowledge structure is to be tested through expert interviews (Phase Two) providing an additional degree of validation to Phase One outcomes.

6.8 Conclusion

This chapter presented Phase One of the study, the development of a literature-informed and expert enriched, knowledge taxonomy for the sub-domain of physical security. Section 6.2 of the chapter discussed the use of, and methodology used to undertake the annotated bibliographic extraction which formed the initial data corpus for this phase of the study. Section 6.3 saw the reviewing, and extracting of concepts accordant with their occurrence measures in texts as representations of repeated themes. Following this Section 6.4 presented the initial findings of Phase One. This included introducing the outcomes of the Pilot Study's Phase Two findings (Table 6.17) to be integrated with the annotated bibliography's findings. Combined this data corpus presented Table 6.18, a taxonomy of physical security knowledge concept categories.

In addition, the chapter also presented Table 6.19 and Figure 6.2, which organise these knowledge concept categories hierarchically to show local connections and structure accordant with the works of Spradley (1979), Eden (1988), Johnson and Christensen (2004) and Bernard and Ryan (2010) (Section 1.8). Section 6.5 provided an interpretation of this Phase's findings. Then Section 6.6 of the chapter acknowledged limitations and Section 6.7 discussed the reliability and validity for Phase One's outcomes. Phase One provided a data corpus and structure to be taken into Phase Two, expert enrichment.

Chapter 7: Study Phase Two: Knowledge category expert enrichment

7.1 Introduction

This chapter presents Phase Two of the study, expert enrichment of Phase One's knowledge corpus for physical security professionals. This phase of the study sought to overcome some of the limitations within the extraction of repetitious key terms or ideas by augmenting the existing knowledge tables (Tables 6.18 & 6.19) and heuristic (Figure 6.2) with knowledge category concepts, principles and practices considered essential for professional work by experts within the physical security field. Consistent with the principle of constructivism, the objective of this phase was to integrate security professional's new knowledge into the existing knowledge system (Table 6.18). It also sought to make explicit new local connections, integrating their views into the existing hierarchical table (Table 6.19) and knowledge heuristic (Figure 6.2). This chapter defines the concepts, principles and theories representing an ideal physical security knowledge system from those working in this occupational area.

The chapter, presented as distinct sections, demonstrates the building of knowledge based on previous knowledge accordant with constructivism (Section 1.8). Section 7.2 presents the participants for Phase Two of the study. Section 7.3 presents the analysis of participant's interviews, including their responses to the methodology and procedure (7.3.1), newly extracted physical security knowledge concept categories (7.3.1) along with knowledge structure (7.3.3) using as much as possible the participant's own words providing descriptive and interpretative validity and consideration of the relevance of the taxonomy to the physical security graduate (7.3.3). Phase findings are presented in Section 7.4, including domain knowledge categories (7.4.1) along with their hierarchical structure (7.4.2). Phase Two is interpreted in Section 7.5; then Section 7.6 discusses the reliability and trustworthiness towards the data analysis and reporting within Phase Two. Limitations within Phase Two were acknowledged and discussed in Section 7.7, where the chapter concludes with Section 7.8.

7.2 Participants

Phase Two sought to enhance the outcomes of Phase One, by presenting the current iteration of knowledge requisites (Tables 6.17 & 6.18) along with its interim structure (Table 6.19 & Figure 6.2) to participating experts. Participants included Des, Kerran, John, Brian, Sharne, Braden, Wayne and Brad (Table 7.1). The procedure sought participant's input to enhance earlier findings through a series of questions (Table 7.2). The objective was to draw out requisite knowledge participants believed was essential for jurisdictional practice yet currently missing from the taxonomy, plus enhance the initial structure of the knowledge taxonomy. As Cohen, Manion and Morrisson (2000, p. 267) state, knowledge is often something generated between people, through conversation (Section 4.3). Accordingly this phase of the study used the research findings to date, along with a semi-structured interview questionnaire to kindle a purposeful conversation regarding the knowledge required to practice at a professional level within the physical security sub-domain or practice area, and its supporting cultural structure.

Table 7.1 Phase Two: Expert's profiles

Name	Profile
Des (Participant 8)	A client relationship manager for a large security engineering organization with over twenty (20) years' experience in the design and evaluation of security risk treatment systems (PPS). His expertise includes security risk management and the technical design of physical and procedural security controls. Des holds an electrician's qualification, electrical technician's qualification and a Diploma of Applied Science.
Kerran (Participant 9)	Senior security consultant with over thirty three (33) years' experience consulting in high level capital works projects. Kerran holds professional qualifications as an electrical engineer and building services engineer, along with formal qualifications in security including Certified Protection Professional (CPP) designation. He has lectured for sixteen (16) years in general facility security at Edith Cowan University (ECU), holding a post as Associate Professor of Security Science.
John (Participant 10)	Security practitioner for over 25 years, now specializing in expert witness assessments for lawyers and their clients in the areas of security negligence and liability. He holds a Bachelor of Science (Security), a Master of Criminology and a Master of Occupational Health and Safety along with certification designations as Certified Protection Professional (CPP) and Physical Security Professional (PSP).
Brian (Participant 11)	Qualified locksmith, security consultant, agent and installer, and lecturer in intrusion and access control systems for a university. He brings 40 years' of security expertise to the study, holding qualifications including Certificate III in Investigations, Certificate IV in Security and Risk Management, Certificate IV in Training and Assessment, a Diploma of Engineering Technology Security Engineering, and an Associate Degree

	in Training and Development.
Garrhett (Participant 12)	A senior engineering security consultant, providing security related planning advice during the early stages of major projects. He worked as a Science Officer for the UK Home Office where he tested and evaluated security technology and is a sessional lecturer for a university.
Sharne (Participant 13)	Security consultant with over 15 years' of experience in the security and consulting industry. He holds a Bachelor's degree in Security and currently specialises in the design of high security technology systems such as access, intrusion - including Type 1 alarms - and CCTV.
Braden (Participant 14)	A security consultant in the Perth and Dubai offices of a large engineering consulting organisation with over 9 years' of security consultancy experience and is an Australian government endorsed security zone consultant.
Wayne (Participant 15)	Holds a Bachelor's degree in Security Science and has over 5 years' experience working in the security consultancy field for a large engineering firm and has carried out projects for both government and private clients across Australia.
Brad (Participant 16)	A security consultant for 21 years, with electronic technician qualifications he specialises in technology. Brad has worked on large capital works projects across the Middle East, Asia & Australia, and also runs an independent security technology test laboratory and associated infrastructure.

7.2.1 Administration of interviews with professionals

Participant interviews took approximately 60 minutes, and comprised 6 sequenced questions (Table 7.2) to guide the phase outcomes. The questionnaire sought participant's thoughts relating to requisite knowledge within the domain of physical security accordant with their professional experience. It also sought their opinion towards the initial knowledge structure (Figure 6.2), and provided them the opportunity to recommend adjustments to the hierarchical table and supporting heuristic.

Phase Two participants were presented with Tables 6.17 (Pilot study: Carried forward knowledge concept categories) and 6.18 (Phase One: Physical security knowledge concept categories) and Table 6.19 (Phase One: Hierarchical knowledge concept category) along with Figure 6.2 (Phase One: Physical security knowledge structure heuristic) to facilitate the interview process. Table 6.18 provided a matrix of physical security knowledge concept categories and their embedded subordinate elements ordered based on their occurrences from texts. All experts were emailed the semi-

structured questionnaire a week prior to their interview (Appendix D), providing time for them to consider the objectives of the interview, questions and supporting tables and figures. The interview discussions were transcribed for later analysis (Appendix K).

Table 7.2 Phase Two: Expert interview questions

No.	Interview questions
1	The table shows the literature extractions top 49 thematic knowledge categories and subordinate concepts. This table was produced through the synergizing of 15 text's salient knowledge categories and subordinate concepts. Is there any knowledge category concepts you would like clarified before we begin? Could you please indicate your support or disagreement with these terms and what you believe the category should be labelled?
2	The knowledge table lists the 49 salient extracted knowledge concepts and subordinate concepts for physical security's body of knowledge, do you agree with these, and if not, what knowledge concepts and subordinate concepts are missing and why?
3	Do you believe any of the knowledge concepts and subordinate concepts should be removed and why?
4	The top 49 knowledge categories have been organised into a hierarchical concept map to illustrate both the structure of physical security's body of knowledge including core and supporting concepts and their relations. This map aims to highlight the knowledge and structure of physical security's knowledge base towards the diagnosis, inference and treatment of security or loss coupled threat concerns. Do you support the structure of this map based on the overall goal for physical security?
5	Do you feel that any of the knowledge concepts or subordinate concepts needs relocating and why?
6	What do you feel are the three most important knowledge concepts for physical security?

7.3 Interview analysis

7.3.1 The methodology and procedure: Participant commentary

While it was not intended for participants to make comment on the study's methodology and procedure, participants were very interested in the study and a number of them made comment on the process in response to the findings presented to them.

At the commencement of his interview Des (Participant 8) expressed a view, from a methodological standpoint, that the literature extraction technique which provided the data to develop Table 6.18 was "pretty good", stating "it does a pretty good job picking up a lot of the key points, some of the them are there because they are common words and not as important, but in order of others it's pretty good". This view was also

supported by Sharne who stated “everything in the chart is relevant”. Braden also expressed such a view, making the comment “everything you have captured, most things, every category that you’ve identified here is something that we have come across in what we do”. Accordingly, from the beginning of their interviews several participants provided an unintended degree of validity to the phase results to date.

Nevertheless, some participants found the general matrix complicated (Table 6.18) and preferred to work from the hierarchical knowledge table (Table 6.19) which they found useful for understanding the knowledge and its organization. For instance, Sharne expressed that Table 6.18 had limited value as the categories, while relevant, had no particular order. He instead saw value in Table 6.19 and Figure 6.2 commenting “they make sense…this is more logical to me”. This opinion was also voiced by Brad who stated, “I find this (Table 6.19) easier to read”. Participants generally found both the hierarchical table (Table 6.19) and the knowledge heuristic (Figure 6.2) very useful in terms of understanding the knowledge requisites and how they fit together within the domain. Both Brad and Kerran supported these representations and further noted that they had not previously encountered anything similar in the security literature. In addition, participants felt the security terms provided were self-explanatory, although Brian expressed that it was difficult to fully comprehend what was contained within the cover term of some of the categories, stating, “as in security we use the terms differently”.

7.3.2 Physical security expert’s knowledge concept categories

An analysis of the interviews shows that while the experts largely supported the knowledge requisites presented, the majority also put forward additional knowledge category areas often distinct to those offered by other participants. This indicates a range of educational and workplace experiences resulting in a diversification of professional knowledge.

John offered the additional categories of *utility*, *fit for purpose* and *aesthetics*. He suggested that security must provide protection while also providing access and use expressing the view that “it is no good having a product and putting it away in a safe so no one can use it, if the security level is such so that nobody can use it (the item), there

is no utility in the security product…you may as well not have it". John considered that utility is often forgotten by security people, emphasizing that "you don't want to have so much security that you can't use it".

Fit for purpose was another concept John felt should be understood well by security professionals. John stated "there was no point having a lock etc. of some sort if it is not fit for the specific purpose". Through further discussion John was asked "are you looking at efficacy for the context, or are you referring to the efficacy of the individual controls"? John explained that he was referring to the efficacy of the individual security components in relation to the context. He suggested that efficacy was a concept hidden in standards but needed to be more explicit and "teased out a bit more in its own right".

> I think it is hidden, because when you start talking standards people think Australian standards or a level. I think it deserved being teased out a bit more in its own right. Because it seems to me so many security systems they have in place either prevent you from using, or take away utility of the product, all you have bought to use and you may as well not have had it. Or they have got some sort of security product that is not fit for purpose, it doesn't work. Yes it's a security product, but it is not really satisfactory and it might be putting closed circuit TV in a bank rather than have a guard on the door… Sometimes these words are not the right word but we don't have the right word in our vocabulary. (John)

John also felt *aesthetics* was another concept category missing from the table, stating for example, "while you want your place to be a prison, you don't want it looking like a prison…that then flows into things like quality of life". In considering Johns views, both the utility and aesthetic aspects of physical security has been discussed in the work of O'Shea (2009, p. 41) who articulated these points as transparent or invisible security. According to O'Shea (2009, p. 41) transparent security means unobtrusive, unrestrictive, and not readily visible, technologies, systems and approaches which address security in the built environment effectively, but in ways that are not readily apparent to the public eye. These categories were supported by environment and review as key aspects of achieving sound physical security where John felt that many people saw security as "a set and forget item".

Finally John felt the cover term *devices* should be removed from the Tables, but this was not fully supported across all participants.

During his interview Braden stated that convergence of information technology (IT) infrastructure is an essential knowledge requisite area, as this is a large part of physical security in contemporary times; especially in terms of enterprise access control. Braden's views were emphasized in reviewed text nine (Section 6.2.1), Physical and Logical Convergence. Accordingly, Braden felt that contemporary physical security professionals must know the fundamentals of networks and perhaps the principles of cyber security, although recognized these as distinct knowledge areas, stating:

> Network fundamentals is essential for a security consultant and for what we do because we need to understand how do networks work and what sort of infrastructure do we need to put in to make sure our systems can communicate. The fundamentals are what we need to know. Do we need to know about cyber security when we are putting those things together – probably not; do we need to understand the fundamentals – yeah? (Braden)

Braden also recognized the role both *project management* and *contract management* have in achieving professional work for physical security professionals, and therefore saw the necessity to include them as categories within the knowledge system.

> A client will come to us and they want to roll out a security project and then we become almost the project manager for that project. On behalf of the client we go out to tender and select contractors, we do an evaluation on behalf of the client and then we will recommend what contractor should do the work. Then when it is being implemented we manage them and make sure they have a program of works that meets the client's expectations and then follow up and make sure it is installed as per specifications… So then that generally includes contract management as well (Interviewer)… Yes, contract management, being subordinate. (Braden)

The necessity for knowledge and skills associated with project management within a physical security professional's repertoire was also raised by Wayne who explained that this represents a massive component of professional practice, particularly as a

consultant. Wayne stated that "if you get into that field…it's pretty well what you are essentially" and identified core skills within the project management domain including tendering, coordinating with occupational groups who install and integrate systems and further liaising to ensure the project elements are completed as per the specifications.

> It can be so diverse, it can be one on one with a client where you are just giving them a report. You can go out individually to tender, that's another big part of it, that whole tender process and managing a contract so contract management. But then a lot of the time, and most of what you do is we are part of a design team with a bunch of other engineers under the builder and architects, and that is probably the biggest aspect of it, delivering projects, that you've been awarded. One on one, but coordinating with all these other facets of design engineering to get a set of documents out to market that can be built essentially. That would have to be in my view the biggest aspect of what we do is being part of a design team. Coordination and liaison. (Wayne)

Furthermore, Wayne felt that physical security graduates needed to be able to read and understand engineering drawings, to have knowledge in ergonomics and also know about software programs for security including building management systems (BMS) and security management systems (SMS). In addition, Wayne also expressed the requirement for sound understanding of electrical theory and switches.

> I find that (electrical knowledge) is another area that it took years to come up to speed with really in terms of how to draw a system up yourself; especially when you need to interface with relays and all those kinds of things. It was very foreign to me when I came here… It becomes so important when you are trying to hand-over or manage a job, that you need to know what has been delivered reflects what is actually on that drawing that you have been given because it might show end of line resistors on that drawing but if you don't know what that equates to in real terms it is hard to justify that it is there or know that it is not there… almost being a contractor versus a consultant and that knowledge. Not necessarily where the wires are going and screwing them in but whether the wool has been pulled over your

> eyes, but, you need to learn a bit to not expose yourself and your company to additional risk. (Wayne)

During his interview, Sharne recognized the requirement for clear jurisdictional knowledge and boundary articulation, to capture what a physical security professional is. Sharne felt that the functional elements in achieving security and its requisite knowledge to be an engineering role, stating "there are plenty of people out there that do risk analysis on theoretical statistical analysis, but wouldn't know the first thing about how to protect something; the whole criminology side is a totally different stream in itself, due to the knowledge required to understand how to protect something".

Sharne explained that the team in which he works includes people from engineering backgrounds as well as those, such as himself, from generalist security backgrounds who need to learn the engineering on the job, "it would make sense to have a degree stream as a physical security professional…if you employ just engineers they don't understand the fundamentals such as crime prevention, environmental design (CPTED), defence in depth, all those principles, they have to learn that on the job". However, Sharne also explained that security isn't simply an engineering discipline, arguing it is a science discipline per se, as unlike engineering there is no specific standard, but rather scientific knowledge to understand the problem and work out a solution.

> One of the issues I think engineering firms struggle with is the first thing they come to us and say where is the standard that tells me how to do this, and when you say there isn't a standard and the answer is I believe this, they struggle with that concept. Because everything they do comes out of a standard, and as long as they are within the guidelines of those standards then they are okay which then relates back to what you've touched on already in terms of if you don't have the theory behind you in terms of how to analyse risk, how to analyse threat, if you don't have the knowledge of how security operations or security management work, again you haven't looked at the risk and you can't analyse a problem then you will never come up with the security solution because you can only see from an engineering point of view.

> We come across that daily with some of our engineer graduates where literally until it is at design development stage where all the concept and scoping have been done and you give them a problem and say right here's the problem this is the solution or come up with a solution to this, not a problem. Go away come up with the schematics, come up with a design – done. But give them that initial problem without all that background and without having solved what we believe the solution should be, they just look at you and can't understand what they are designing. (Sharne)

While Sharne acknowledged diagnosis of the security problem to be fundamental to being a physical security practitioner, he declared that it is just the beginning, as they do everything in his team, from risk, threat assessment, scoping through to detailed engineering. However, when it comes to detailed engineering issues such as vehicle ratings and penetration testing "I am not a structural engineer", so we will engage the requirements of a structural engineer. "but we would like to think the security consultant has been with, and carries the design through all the way, and doesn't just rely on the engineer". Sharne explained that, in the designs they put forward, security (the team) takes the lead, and seeks input from the engineers, architects and others to do their specialized tasks.

> Other consultants are different, plenty of consultants that are out there and call themselves physical security professionals, yet in some cases their primary role, and a lot of our clients can be that way, they will do the initial risk assessment but when it comes to technical design they will get somebody else to do it. That is for professional reasons, for commercial business reasons for a whole range of skill limitations. There are other consultants that will do a design up to concept level and get the contractors to design and do all the calculations and all of that. I don't think that is the right way to go, if it is a developing profession, which it is, we should be setting up training and educating our graduates to understand all of that information and to produce all of the calculations they need to do whether it is, designing a CCTV system or understanding the broad calculations for vehicle and bollard protection. (Sharne)

Supporting clear jurisdictional boundary or focus for security professionals, Sharne believed that physical security professionals need the capacity to take the security project from risk diagnosis right through to the treatment implementation phase. He also expressed additional knowledge requisites to include the fundamentals of project management, stating "without it you will never implement anything successfully". In addition, emergency management fundamentals were required, acknowledging this is a separate profession, but stating "it makes you aware of the codes (building), emergency procedures, what you should do, what you shouldn't do, you need those fundamentals".

> You need those core fundamentals, you don't need to know any more than if you are providing physical security measures for a building well you better make sure you have thought about the emergency and the BCA (Building Codes Australia) requirements and fire. You need to know enough to know when you are stepping into somebody else's realm or to bring those people in where appropriate. If you don't have that fundamental background how do you know that. (Sharne)

Sharné's view of the nexus between emergency management and security has been discussed in Craighead's (2003, p. 21) text High-Rise Security and Fire Life Safety, which acknowledges that while security and emergency management are two different disciplines at times these subjects are so closely interwoven that they appear to be the same. Sharne also saw the necessity for fundamental knowledge in the realm of cyber security…"at a fundamental level you have communications and networks and they become rudimentary to what we do. In our industry (physical security) we are seeing more and more convergence, primarily due to do the fact that electronic security systems that we spend most of our time designing are now sitting across networks". Sharne also proposed the requirement to monitor what is occurring within the treatment system as an essential capability to have, adding it to his list of missing knowledge items.

Further adding to the list of knowledge inclusions, Garrhett commented that management, not project management or security management but professional process management, was important knowledge to have within a consulting practice cover term. According to Garrhett, many graduates from security programs do not actually know the

process which consultants go through, from the proposal stage all the way through to commissioning a product.

> There is the proposal stage but all the way up to commissioning, like writing the design brief, doing the detailed design, what are the different stages you can do, a concept or a master plan and then you do a 50% design then you have a 100% design and then you've got reviewing shop drawings from the actual installers and then you've got commissioning and things like the 'fac' test, the factory acceptance test. So all that process is really beneficial to already have an understanding of because even if you are not a consultant like us but if you are working in a firm you are, or will be communicating at that level, if you are designing a system yourself and then engaging the sub contractor yourself, you are still going to go through that process… I'm just talking about the process and the different processes.
>
> There is another one called FEED, which is Front End Engineering Design then there is EPCM (Engineering Procurement Construction Management), and we have to deal with all these different processes that do share similarities but also differences and fit in our program and what we do into that and what the client wants. I think having an understanding of the different engineering processes that we have to go through could be beneficial… And they are different across different industries as well. If you do a FEED for resources and power and do a FEED for the built environment they have different gates that the project has to go through so they have different drivers. I found that really interesting. So you are applying your security knowledge and then you've got a different industry and they treat the process differently. (Garrhett)

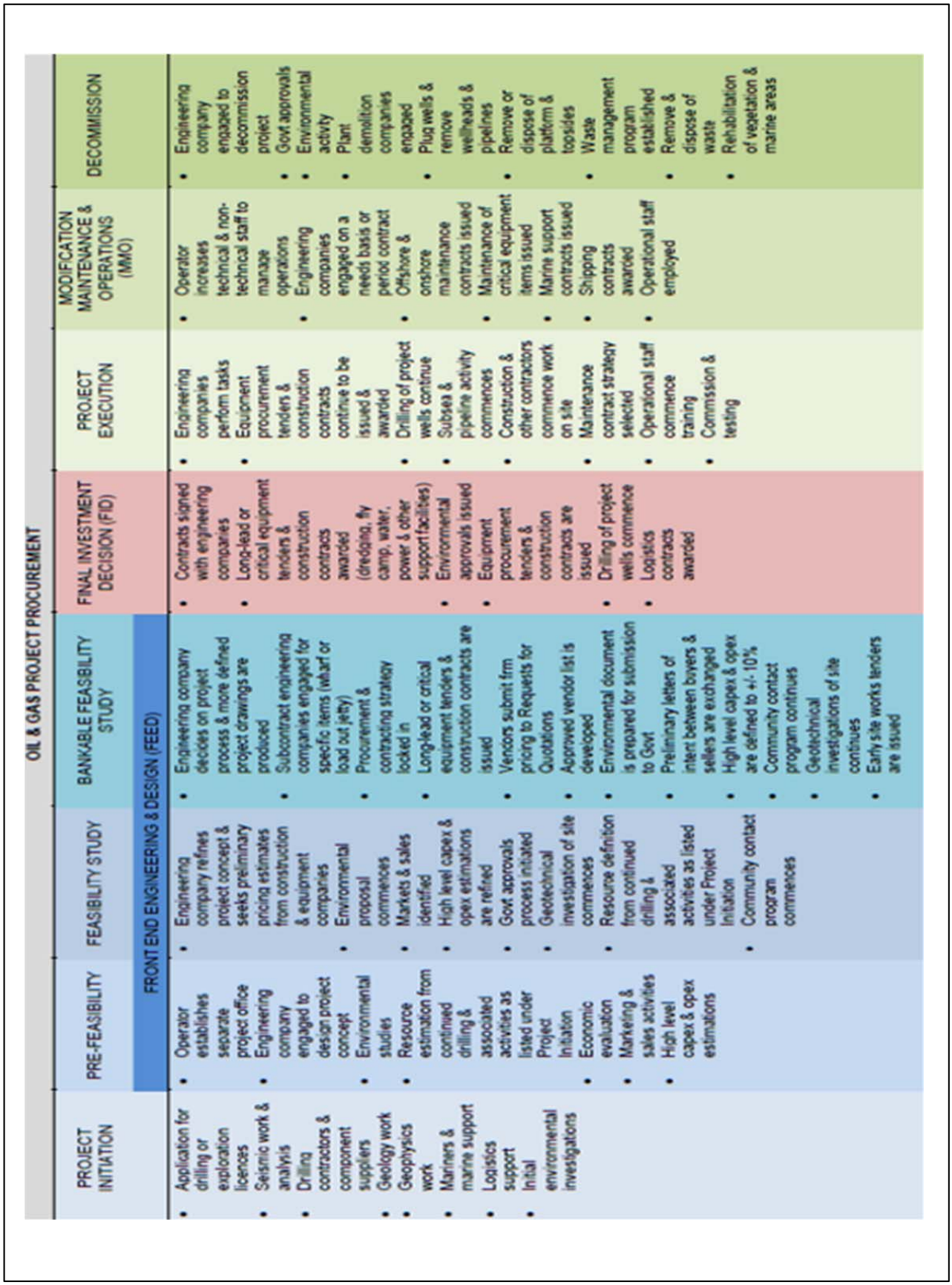
Garrhett explained that this refers to knowledge of the engineering process or consulting practice. For physical security professionals, Garrhett expressed it is essential to understand in principle the industry processes and where their knowledge fits in. Garrhett provided two tools to emphasize his view pertaining to such knowledge requisites. First, Table 7.3 indicates his version of sequential phases and process undertaken to achieve a physical project outcome. This is supported by Figure 7.1

presenting graphically the project design phases from project initiation through to decommission.

Table 7.3 Garrett's front end engineering design process phases

Front End Engineering Design (FEED) Process		
Phases	**Themes**	**Outcomes**
Phase One:	Enabling works	
Phase One(A)	Security Survey	Undertake a security survey for the XXX where this interfaces with the construction of the XXX expansion and provide recommendations
Phase One(B)	Enabling Works Plan	Provide a plan on how to divert existing security services at the XXX to allow the enabling works for the XXX expansion to be carried out.
Phase One(C)	Temporary Works Plan	Provide a plan on how to provide temporary security services for the XXX during the construction phase of the XXX expansion
Phase Two	Security Risk Assessment	Update the security risk assessments for the XXX and XXX to accommodate the XXX new expansion areas.
Phase Three	Concept Validation	Prepare these concept designs, based on tried and proven security concepts, which will provide the 'building blocks' for future stages.
Phase Four	Schematic Design	Prepare these schematic designs based on the approved concept designs.
Phase 5	Detailed Design	Provide a detailed design with updated specifications and drawings.
Phase 6	Tender / Construction Docs	Prepare tender documents for XXX to issue to the market, carry out a tender assessment of proposals submitted by contractors and provide a report
Phase 7	Construction Administration	
Phase 8	Security Procedures	Update the existing XXX security procedures which have been affected by the XXX expansion.

Figure 7.1 Garrhett's front end engineering design process heuristic



Combined these tools show additional professional knowledge required by persons working within the higher level physical security domain in addition to their core security knowledge. Such views were also expressed by Des who considered it necessary to know the *design process*, and that such knowledge is a significant requisite knowledge area for physical security professionals.

> It becomes quite important to a grad to understand that you come in and get given a job. The management and the process of delivering that job is something they need to learn. There is a point with a task, we write a proposal, we win a job, it lands on someone's desk it's the management of process. Understanding how I get from the point of having this (proposal) to actually achieving the deliverable. If you're talking about teaching someone the education process of how to work in this industry there is a general process around, you are going to be working either for a business or for a client, you are going to be providing a service in house for that business, you might be employed by or on the security team, and you are working in there or you are working for someone that is outside providing that service to that organisation. Either way, at some point you are given a project and there is a process, there is a way of managing, I suppose it's almost around time management and understanding how to achieve a deliverable, it's really difficult to put some wording around that.
>
> You must know and understand all these sorts of things, if you don't know how to, it's almost like you give someone an assignment, how do they plan and managing the delivery and the output of that assignment. In itself I think it is something that, it is being able to get that context around what it is your being asked to do, understanding from the early days of what is the key point… what are the deliverables? You do not run off and do what you think needs to be done, but actually delivering what you have been tasked to do. That in itself, from a security point of view, is absolute, because if you haven't got the context and don't understand the task we end up, the other word the term I use a lot its around mitigation, security is around what we do and have I achieved, we talk about mitigation strategy in the end we want

> to look back and measure, and did we actually mitigate that risk, did we actually achieve what the client needed done? (Des)

"So you are looking at what is the objective, do we understand the objective"? (Interviewer):

> Yes, do we understand the objective, do we know how to plan to achieve that objective, do we know how to implement the process to achieve the object and do we know how to deliver it? To me that is a really important thing. Otherwise you can quite often give a person or client an outcome that doesn't necessarily meet their needs. It's a bit like, if I have a person with a security issue and if you sat down at a table and someone said we should start talking about cameras here and access controlling this door and I'd sort of go well can we move the plan out of the way, can we talk to you about what actually is the problem, it is caused by what risks, what's your threats and risks. So going back to understanding, you get an outcome that delivers on that… Its then understanding if the problem has been diagnosed then what's the plan, so your doctor might say well we're not going to put you on aspirin because your blood is already thin, so it's a matter of how do you interpret, its understanding the process that you need to go through, to interpret that evaluation and know how to plan the way to get to the point that you have got the correct treatment process in place and therefore you get the desired outcome. (Des)

Des and Garrhett both considered that the *engineering design process* should be a major knowledge category area covered in security education as graduate physical security professionals must understand this. This position is congruent with the written work of Smith and Brooks (2013) within their security science text (Text 13, Section 6.2.1). These authors explained that physical security science uses both scientific method and its extended methodology – the engineering design process - to achieve security related objectives. They show the correspondence between the two methodologies through Table 7.4.

Table 7.4 Scientific method versus engineering design process (Smith & Brooks, 2013, p. 5)

Scientific Method	**Engineering Design Process**
State a question or problem	Define a problem or need
Gather background information	Gather background information
Formulate hypothesis; identify variables	Establish design statement or criteria
Design experiment, establish procedure(s)	Prepare preliminary designs
Test hypothesis by doing experiment	Build and test a prototype(s)
Analyse results and draw conclusions	Verify, test, and redesign as necessary
Present results	Present results

Bracing the knowledge base of physical security professionals, Garrhett highlighted the fundamentals of *mathematics* and *physics* that underpin the security solution as an enabling knowledge requisite for physical security professionals.

> Having an understanding of the physics, of how this technology works, really gives you an understanding of if it's going to work or not, and how it is going to integrate with all the other engineering services. "So they don't necessarily need to be engineers but they need to understand the principles behind what the engineer is telling them" (Interviewer). Yes, and that will let you communicate with the product suppliers as well, because the product suppliers generally are very knowledgeable as far as the science and math goes because they and the installers, generally have a really good foundation on the physics behind their technology, either because they are installing it or selling it. And when they are trying to explain some new thing that their product does and why it is better than the other product, they have to prove it almost and you can do that through testing, but if you know the science behind it you can sort of understand how that works or its limitations.

> So when you are looking at a bit of technology, without just reading the sales pitch to it and knowing actual the mechanics of it, it is really beneficial, because then you can ask questions and say well with this last product did xyz because of this wave or this bit of technology, or use this theory or whatever, and how does that differ from here, and you just add to that foundation as the technology develops and I think that is really important…for me I think that technical, the pure fundamental science in physics and technical knowledge is the most important trait to have and I would be looking for someone who had that skill first because I think it is easy to teach the theories (Security) on top of that than it is to teach someone the science behind it. (Garrhett)

Des recognised the importance of *safety* as a knowledge category, stating that "security and safety are inextricably linked, you can't talk about one without the other". This view was supported by Wayne who stated that "safety is such a huge component now…everything starts off with safety, every discussion, your safety and design is one of the biggest requirements around projects; you have to show how your design is inherently considering safety, so you don't have a panel up at 4 meters on the wall it's at 1.8 so you don't have to bend, ergonomics all those sort of issues".

Within the printed domain, the nexus between security and safety is well documented for example, Tooma (2011, p. 1) asserts their connection lies in their underpinning principles of well-being, along with the risk management approach used to achieved their outcomes. While recognizing security and safety as distinct disciplines, Tooma's (2011) work asserts that rarely does a major incident in one context not impact on the other (p. 1), even though this nexus through occupational security law is still in its embryonic stage (p. 50).

Des also emphasized the requirement to understand the basic philosophy of security, expressing that

> You can learn all you like about CCTV and access control, but if you don't understand the actual basic philosophy of security and its application then the rest of it becomes irrelevant. Because to me the technology and all a lot of these other things that we have got in here are (Table 6.19), basically outcomes that fall off that process so I have seen clients that have spent an inordinate amount of money and not fix the basic problem that they have. (Des)

Des's views correspond with the American Institute of Architects' (2004) security design planning framework. In their text, the Institute (p. 40) emphasizes the theoretical elements of CPTED, situational crime prevention and spatial zoning principles along with the functional elements of deterrence, detection, delay and response (defence in depth) to form a design framework or philosophy for security planning. Within this framework the individual security products merely achieve the broader goals.

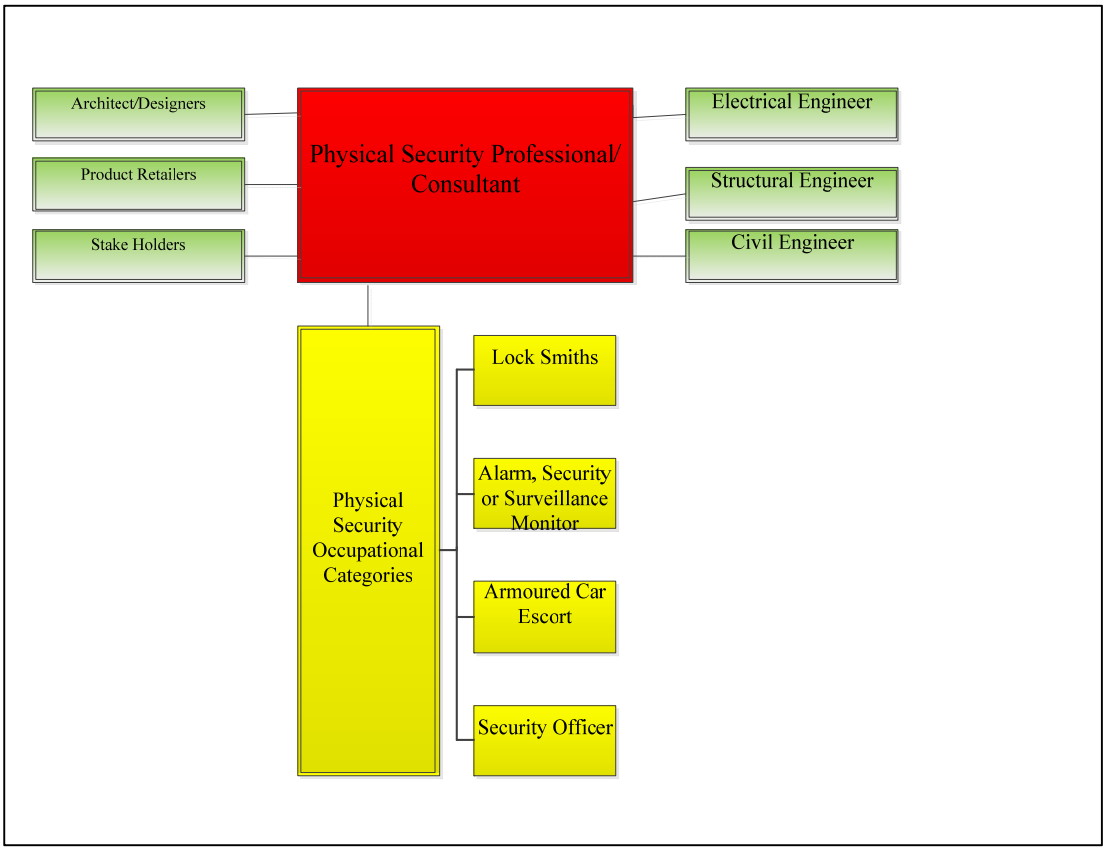
Des expressed that physical security professionals need to understand where their specific knowledge and skills fit in the broader context of a security solution. They then need to be able to communicate clearly "in an up and down manner" with different people regarding the various knowledge inputs. Des expressed the requirement to be able to write and communicate (verbally) technically with the structural or civil engineer, yet also communicate in a non-technical way to the client, and other stakeholders that have got to be involved in a project control level.

> Let's just use that as an example, let's say we are talking about a secure fence, I as a security consultant, will talk to our client about the type of delay we need to achieve by that fence and we will define that in three ways - under, through and over, simply as that. So each one of those has to be treated, the through bit is, but it still has to be physically strong enough to withstand the environmental conditions that it is in, whether that be wind, lightning, whatever, so you've got your structural engineer and your civil engineer, they become critically important to the design of the fence.

> You've got your fence manufacturer that has a product that you want to use and understand that.
>
> So what I see, we set a criteria around the performance of the fence, I want the face of that fence to be anti-scalable, so I will talk to the potential architect or the person that is designing the fence about how we achieve that, we know that we want limitation penetration and that is around the fence material so we talk to, we know the fence has to stand up and it either has to have some sort of cowl or topping so from your civil engineer, your structural engineer, your fence manufacturer and your fence installer, all of those sorts of people in here, the knowledge that I need to have is not only the objective of what I want, but who do I need to talk too?
>
> So in the process I need to be talking to a structural engineer, civil engineer about the ground finish, how do we stop the anti-tunneling, how do we get the water away for the longevity of the fence, electrical engineer, we've got the lightening protection issues associated with the fence, the manufacturer – how do we detail so we get an anti-climb finish on the fence so that nice smooth finish and then the installers. In terms of the body of knowledge, I suppose what I'm trying to get to is that I have an objective, my way of knowing how to get to that objective is quite complex and it needs to involve other people so I need to know who I need to involve and at what stage of that process to actually achieve the outcome. (Des)

The views of Des and other participants enhanced the occupational strata graphic (Figure 1.1), adding horizontally other professional participants into the occupational system required to achieve a high level security solution. For example, as a reconfigured diagram, Figure 7.2 shows how Phase Two's participant's views add to the system of professionals and occupations that functionally achieve a Physical Protection System (PPS).

Figure 7.2 Security professionals/consultants and their supporting occupational strata



Des's articulation of a broad stakeholder engagement to achieve professional security outcomes is consistent with Freidson's (1970, p. xvi) and Abbott's (1988, p. 8) discourse on medicine and other professions. Freidson notes that drawing on the sciences, medicine has developed into a very complex division of labour, organizing an increasingly large number of technical and service workers around its central task of diagnosing and managing the ills of mankind. Abbott's (1988, p. 8) work conveyed a similar view, expressing that the physical techniques of the professions may in fact be delegated to other workers but the knowledge sitting around the process is of abstract nature and the role of the cultural professional. Such articulation may indicate a progression in professional maturity for physical security in terms of a higher occupational role, one that diagnoses the concern, and then through abstract knowledge coordinates the design and implementation of the treatment plan.

During his interview Brian did not like what he believed to be the incorrect use of *door furniture* as a category. According to Brian:

> There are three things on a door, not in any order, there are locks then there is furniture, then there is hardware - that is it. Now locks can incorporate the physical lock as well as the cylinder, which is a subject on its own, furniture being handles. Then the hardware is everything else on the door that is not the lock and the handles, therefore hinges, door closes...So hardware, and that also comes down to door numbering, identification or signs and if you look to go to a scheduler who looks after a building, when it comes down to locks and things like that there is hardware, furniture and locks. (Brian)

Brian's professional standing as a security professional and qualified locksmith saw the categories changed to reflect his expertise. Brian also expressed the necessity to have a category called *utilities*.

> Power is important but under that, rather than power put utilities, because if you knock out any utility to a building, they might rely on gas, water, the water escaping, you do any of those things then the company is not functioning, depending on what the company is, so rather than putting it down as one thing like power… Instead of electric power make it broader, and say utilities… then break it up to define what utilities are. (Brian)

According to Brian utilities need to include gas, water and electrical, along with its facilitating infrastructure. Kerran's views concurred with Brian's comments, making the point that security graduates need to understand how to thread engineering services through a building. Stating, "every time you thread these through a building you are creating apertures for those to go through, light fittings in ceilings, mechanical ducts and the like, all of those (apertures) are weak links in the chain". Kerran also noted that there needs to be some basic concepts in here relating to structural strengths (delay), it is not only the strength of the barriers themselves but all the fixings and managing the apertures. To a limited degree these issues are discussed by Craighead in his text High-Rise Security and Fire Life Safety (2003). However, Kerran is expressing a requirement for deeper knowledge beyond what this text offers.

Kerran also stressed that security teaching should adopt a narrative approach, that is using contextual examples, to demonstrate key points. He then used the narrative

approach to emphasise how physical security professionals must understand the compatibility of design elements, as the compatibility of design elements are 90% of where physical security falls down. The way the locks are fixed to the walls, the way hinges are bolted into the walls needs to be understood by physical security consultants. Kerran gave the example of Oak Park Heights, to demonstrate his point.

> Very late in the process they decided to build this secure wing, so they put the block up there and built a basement with 20 cells in it, it had a big open area in it…. What happened was they needed it done in a hurry and the architects building it were so busy they bought another firm in to design it, they got pieces of drawings and goodness knows what from other people but they didn't understand what they were doing, the 20 crims walked in, looked at the door hinges and said thank god I'm here. So they all one by one ordered paperbacks from the library and then one particular afternoon they all came in and put three paperbacks in the jam of each door and when you slam the door the hinges go like that, the door could no longer be locked and closed because the door doesn't fit in the frame anymore coz the hinges had been sprung. (Kerran)

According to Kerran, much of physical security is about experience, being exposed to testing and then dissecting what has worked and what hasn't. *Testing* was also a knowledge area raised by Brian, including project acceptance testing and compliance with technical specifications testing, where, consistent with the writings of Smith and Brooks (2013), such testing requires the application of the scientific method. This was a theme strongly supported by Brad. Brad expressed the necessity to recognize and teach scientific method**,** stating "if I had to go and look at the material resistance of something I would start by talking to a concrete contractor, getting some reo and having a dirty great hunk of concrete poured into my back yard that I'd hammer my way through over a period of time and I'd try a number of different tests. That is what I would do" (Brad). Kerran supported this stance, pointing out the requirement for a clear methodology to solve the problem, be it global or micro:

> You have got to look at the global problem and then you work your way down in your solutions so you can't ignore the bolts and nuts but you don't

> start off with the bolts and nuts, you start off with the context. The whole facility contextualization, and then you reduce it down to each element that you are doing and then you look at those in detail but unless you get that bit right you will never get this bit right and that can be taught (method) in the body of knowledge. (Kerran)

Again, consistent with Smith and Brooks' (2013) text, the necessity for comprehension of the scientific method and the engineering design process as knowledge categories for future physical security professionals was a well-supported theme. Kerran's professional process view, in principle, supports the general structure of the hierarchical table, where knowledge areas are hierarchically divided into diagnosis, inference and treatment, specifically stating, "you don't start down here, you start up there… It is actually a methodology; it's an approach, a concept of conceptualising security solutions almost".

Following on from this, Kerran also believed *audits* needed to be added to the knowledge categories stating:

> Audits are about establishing a set of base levels, you are not just looking at against a threat, but you are seeking base levels, this thing here does this comply with this, will that deliver this, that is a security audit where you are going in micro detail and assessing, reviews are a much more high level of process that is being undertaken, surveys tend to apply more to management than the physical security, audits look at everything and reviews look at what have we got relative to the threats that apply. (Kerran)

Brian also expressed the desire to change the category of *safes and vaults* to reflect *security containers* more broadly, arguing for the category of security containers to include drugs safes, and secure envelopes as well, stating:

> If we are talking safes and vaults then, rather than safes and vaults, there are different types of safes and vaults, one of the terms we have been using was security containers. As well as being security containers it will also look at for example fire security and it will take care of drugs, it will take care of

> money, bullion, there are different types of construction and types of safes, depending on what you are trying to protect and how. For arguments sake, if you have a fire safe, there are two different types of fire safes – one for paper and one for data because the humidity is different, so if you had a title, security containers, then that would cover them all. (Brian)

Brian further indicated that as a security professional within his area of expertise he deals with the possible threat of *espionage*, yet this was not an extracted threat category. Thus Brian advocated for its inclusion.

A category refinement which was suggested by both Brad and Kerran was that *planning and design* should be called *security planning and design* to reflect the specific nature of the security role within any broader project context.

Additional categories arising from the interviews are presented in Table 7.5.

Table 7.5 Phase Two: Participant centred concept categories

Physical Security Knowledge Category Areas			
Utility	Quality of life	Fit for Purpose	Aesthetics
Environmental conditions	Review	Context	Proportionate Level
Building services	Emergency management	Project management	Monitoring
Network fundamentals	Contract management	Material ratings	Security management plans
Security design process	Physics	Computing fundamentals	Acceptance testing
Consulting practice	Engineering principles	Engineering drawings	Electrical theory
Ergonomics	Building Systems-management systems /Security management systems (MS-SMS)	Professional liaison	Fixings
Integration	Design compatibility	Security planning and design	Utilities: Hydraulic/Power/ Mechanical/Gas/Water
Ducting systems	Openings/protrusions	Security containers	Drug safes
Fire safes	Secure envelopes	Technical specifications	Espionage
Door Hardware	Cyber security	Mathematics	

7.3.3 Physical security expert's hierarchical structure

Participants reflected on the hierarchical structure of the knowledge concept categories as presented in Table 6.19 and where appropriate recommended the placement of their additional categories and the movement of existing categories to reflect an order more meaningful to them.

For instance, Braden thought that locating *CPTED* near technology was incorrect suggesting it was more related to *situational crime prevention* and *defence in depth*. Kerran clarified this further stating "it's not (CPTED) a physical environment, it's a planning environment…You're planning and designing here, CPTED should be linked to the planning and design because it's a planning exercise, you can't apply CPTED after the event, CPTED is applied at that time… It has to be built in".

> It is physical but the principles are applied at the time of design, if you don't then what you will be doing is building, one of the classics is architects like to put reveals in buildings because they give shadows, but then people stand in them and they can't be seen and they are a threat, so what you end up doing is building a wall in there or putting something to stop people going in after the event, so all of the context CPTED in two parts but it is through environmental design, it really should be up at the design process rather than the physical process because once you've got those principles right the physical element falls out. That definitely should be up here because it is a design process it is not, when you read the book on CPTED, very rarely does this book give you detail of physical construction attributes, it's all these are the principles. (Kerran)

Again, Kerran's view reflects in principle the American Institute of Architects' (2004) framework for security design. As expressed, the Institute's (p. 40) text emphasizes a design framework or philosophy for security planning through the coupling of CPTED, situational crime prevention and spatial zoning principles along with the functional elements of deterrence, detection, delay and response (defence in depth). Braden also saw *security surveys* and *risk* to be associated stating "usually if you are doing a survey it is part of the risk process that you are undertaking". Noting the place of *risk* within

the hierarchical table, Braden stated, "I see you have risk up the top; that sort of includes everything so that is probably right; it all makes sense". This positioning is consistent with Somerson's (2009, p. 61) work, which explained that while some people confuse a security survey as being synonymous with the total function of risk assessment, it is actually an ingredient in performing a risk assessment.

John expressed that *utility* as a category would sit beneath *law* in the hierarchy along with *aesthetics* and *efficacy*. This saw these knowledge categories sit within the planning elements of the knowledge corpus, as John stated, "they are fundamental planning principles".

Nevertheless, John noted that there may not be a single place for such knowledge to be located, as it may sit in multiple places. In addition, John acknowledged that this study, due to its uniqueness, is the first iteration, and therefore "much knowledge placement will be provisional". He also did not know where to locate *environment* as he perceived this as spanning many categories, but ultimately saw it as a planning category. John stated that "physical security is not a linear process…and we don't really know in hierarchical terms where everything sits…at the moment we have just got them all in a big bundle, in a big bucket and they are only sitting where they are by virtue of something sitting over or under it, not because it is placed by order of importance…this sort of thing (study) is well overdue…we (security) don't have a framework to work from".

Brian noted that *espionage* as a category should be located under *threats* and that *review* should be a superordinate category as it covers almost every aspect of the security concern, stating "I would just review everything". He also expressed that *utilities* should be a broad category then falling underneath that, the specific utilities such as gas, water and power. Kerran considered that *audit* needed to be added with *survey* and located together as part of the broader planning side of things, stating "together they are different things but all have the ability to influence what comes out of it".

> All of them are analysis of the existing stuff that is in place relative to a threat, what they do is these are underpinned by different outcomes, the audits are you establish a set of base levels, you are not just looking at

> against a threat, but you are seeking base levels, this thing here does this comply with this, will that deliver this, that is a security audit where you are going in micro detail and assessing, reviews are a much more high level of process that is being undertaken, surveys tend to apply more to management than the physical security, audits look at everything and reviews look at what have we got relative to the threats that apply. (Kerran)

7.3.4 The physical security graduate

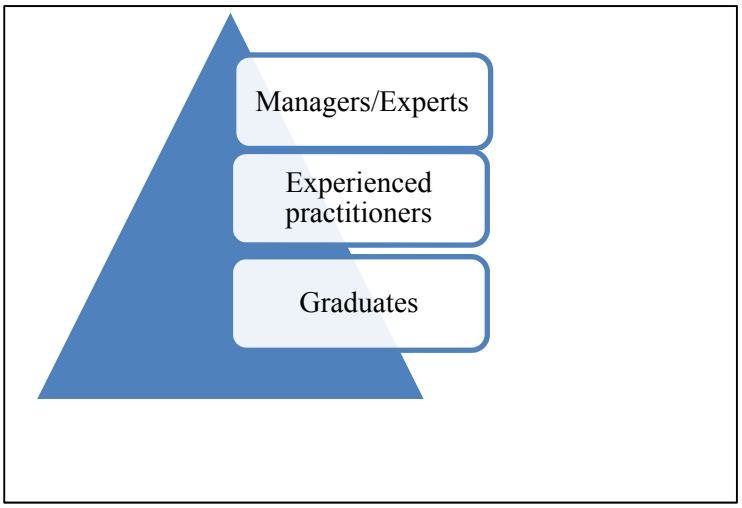
An analysis of the Phase Two interviews highlighted that graduates require fundamental understanding across the various knowledge category areas, as well as an understanding of how the various knowledge categories relate to each other, to produce a constructed outcome to mitigate risk.

However, further professional development within an employment context is essential prior to reaching a competent level of practice. Wayne experienced such development and stated that "as a graduate you come in very much at an apprentice level, you are starting right at the bottom, you won't be doing design and client liaison to start with. You are probably going to be doing colouring in and counting". The professional apprentice theme continued throughout the interview process. Kerran explained that when he ran a large security engineering company, graduates had to do four years before they could see a client, "in case you said the wrong thing". However, according to Kerran it usually took five years before a graduate was allowed out on their own stating that "they need the acquired knowledge of an old tradesman, they need mentoring".

This was a theme encountered earlier in the pilot study where participants articulated that the focus of physical security education should be towards producing graduate level persons not competent professionals. For instance, Jeff (Participant 5) expressed that the profession of security needs to have a staged hierarchy that allows graduates to be developed further post-graduation; stating "a medico goes out and becomes an intern, and accountant goes out and becomes a junior accountant, a manager goes out and becomes an advisor or something like that. They go into graduate jobs and then they progress upwards…if security is going to progress as a profession we must prepare

people for graduate jobs". This discourse again supported the security professional's stratum Figure 7.3 (5.5 in the Pilot study) which sees knowledge and experience in graduates build over time, and with these professional progression.

Figure 7.3 The security professional's stratum



Brad expressed that graduates required fundamental knowledge of the category areas represented in Tables 6.18, 6.19 and Figure 6.2, stating:

> Fundamental knowledge is really important, and when I say fundamental knowledge, if you sit someone down and you say - you put a lens on a camera, you connect the camera to a wire and power supply, you connect the wire to a monitor and you get a picture out the other end, the take home message from that, a lens, a camera, a wire and a monitor will give you a picture from there to there but when you change the technology that wire may not exist anymore and you might have a camera that has a built in lens and you might not have a monitor you might have a computer and all of a sudden the wheels fall of. I think it needs to get down to a more fundamental understanding, which is – we take a picture, we break it up however we break it up, it gets reassembled at the other side and it gets displayed, and that transfers across all generations of technology, current and future.
>
> The best part about that fundamental knowledge is the person can then turn around and say well I actually don't understand how that picture gets from

> there to there but I know that fundamentally it gets broken up and it gets reassembled so I need to go and learn how this bit of technology works to get this bit to this bit, whereas if you just say lens, camera, wire, monitor, they say hang on we don't have monitors anymore and we don't have wires any more I'm lost. I saw a specification not that long ago that said you shall use 5 mega pixel digital cameras and record them on SVHS video recorders. Fundamentally incompatible technologies. It just needs to be that more fundamental understanding, it's like an alarm system, you've got a switch, or a detector but fundamentally it's just a little circuit and once you understand that it's transferrable to all future technologies. (Brad)

This was also supported by Garrhett who stated that the fundamental knowledge of the underpinning *mathematics* and *physics* for physical security was really important. According to Garrhett, "if you take someone who has a really good understanding of the science behind these technologies, they will do very well because then they can just add, they have got that underlying understanding of the technology, because at the moment we are very technical system based, having that grounding is very important". Garrhett stated that as an employer of graduates for a large engineering organisation "I think that technical, the pure fundamental science in physics and technical knowledge, is the most important trait to have and I would be looking for someone who had that skill first because I think it is easy to teach the theories on top of that than it is to teach someone the science behind it".

Sharne supported this stance also, stating that graduates need the knowledge fundamentals and this includes the fundamental knowledge to take the project from risk level right through to the implementation phase, stating:

> There are people who will consider themselves a physical security professional but under physical security they are talking in the risk-threat assessment sphere…if you are going to be a physical security professional you need to be able to take it from risk level right through to the implementation phase. (Sharne)

Across the interview participants, the most important knowledge requisites for graduate physical security professionals were the risk based approach (Des), along with setting the appropriate level of security in the planning phase (John & Kerran). Then understanding the technology (Des) including the physics that underpin technology (Garrhett) and the methodology that is embedded into all stages of the security project, from diagnosing the real risks and articulating the strategy and design (Kerran) through to commissioning the solution (Brad). An analysis of each participant's interview transcripts highlighted that physical security graduates need to have a broad fundamental knowledge basis, from security or facility project conception through to commissioning and that this knowledge is braced by excellent communications skills, both verbal with the ability to speak clearly and technically with clients, as well as the ability to communicate clearly in writing to produce high quality reports. It was also highlighted by Kerran that individual graduates may not use all they learn at university, it is about a holistic base:

> I've always said to the graduates when you come out with the degree, if you use 5% of what you did in your degree, doesn't matter if its engineering, security whatever, you use 5-10% if you are lucky, and in my notes my degree if I use 5-10% of that, but what I did was I learnt the theory to take a problem and come up with a solution. (Kerran)

7.4 Phase Two: Findings

Phase Two investigated knowledge concept category areas that, accordant with their professional experience, participants believed were missing from Phase One's analysis (Tables 6.18, 6.19 & Figure 6.2) and the Pilot Study findings. Phase Two sought to respond to the question:

What are the implicit knowledge category areas, and instinctive structure used by security [experts] in achieving physical security risk mitigation not extracted from the literature critique?

7.4.1 The domain knowledge categories for physical security

Participants highlighted an additional 43 knowledge concept category areas or subjects within categories (Table 7.5) they considered essential knowledge for future physical security professionals. These additional 43 knowledge requisite categories combined with those from Table 6.18 led to the development of a Phase knowledge concept category table (Table 7.6) and their supporting knowledge elements. This process resulted in a matrix of 98 knowledge concept categories for inclusion as a system of knowledge for physical security professionals.

Table 7.6 Phase Two: Physical security knowledge concept categories

Physical Security						
Security	Law	Facility contextualization	Assets	People	Data & Information	Property
Infrastructure	Attack	Adversary	Threat	Terrorism	Crime	Safety
Loss	Espionage	Risk	Security surveys/ reviews/audits	Prevention	Control	Security planning & design
Architectural drawings	Aesthetics & utility	Environmental conditions	Security theory & principles	CPTED	Situational crime prev	Defence in depth
Security management plans	Security Level	Consulting practice	Movement control	Engineering design process	Engineering principles	Services & utilities
Electrical power theory & principles	Gas	Water	Surveillance	Technology	Detection	Alarms
Facility/Building Security	Equipment	Sensors	Intrusion	Fire	Lighting	CCTV
Field of view	Lenses	Resolution	Contraband Drugs	Integration	Network fundamentals	Security management systems
Cyber security	Building systems	Openings/ protrusions	Ducting	Delay	Structural strengths	Walls
Windows	Access control	Barriers	Fencing	Glass	Fixings	Doors
Door hardware	Door furniture	Locks & cylinders	Security containers	Vaults & safes & envelopes	Standards & technical specifications	Response
Guards	Procedures	Interruption	Force	Ergonomics	Design compatibility	Efficacy
Analysis & evaluation	Mathematic	Physics	Factory acceptance testing	Site acceptance testing	Emergency management	Systems theory
Costs	Report writing	Review	Monitoring	Project management	Contract management	Professional liaison

7.4.2 The hierarchical structure of physical security's knowledge

Phase Two's knowledge concept categories (Table 7.6) were used to develop Table 7.7, a Phase hierarchical table of superordinate and subordinate knowledge concept categories along with their local connections. Facilitated through inductive then deductive analysis of participant interviews, Table 7.7 presents physical security's hierarchically organized knowledge structure. This knowledge system includes core content and supporting professional knowledge to facilitate professional work in the area of crime and loss prevention within the domain of physical security.

Phase Two findings indicate that physical security's knowledge base includes a minimum of 98 superordinate and subordinate knowledge concept categories as distinct, yet interrelated theories, concepts, principles and elements (Table 7.6). In addition, these separate areas of requisite knowledge are connected, that is, they have internal relations according to their contribution with the professional goal, and organized on the basis of a single semantic relationship, represented by the word security (Table 7.7). Such findings support that this content has internal relations that as a systemized structure can be mapped and presented for enhanced reception learning (Table 7.7).

Table 7.7 led to the development of Figure 7.4, a physical security professional's knowledge heuristic representing core knowledge areas, their subordinate elements and their qualitative derived local structural relations. Figure 7.4 represents the latest iteration in the development of a domain symbol for communicating concept categories and their relations forming a physical security body of knowledge heuristic as a shared paradigm (Section 1.8). For novices and security educators, Figure 7.4 highlights the requisite individual knowledge elements within a physical security professional's knowledge system, their connections and structural relations with other knowledge elements. Such a heuristic informs of the requisite knowledge elements within a physical security professional's knowledge system necessary for professional practice. In addition, it enables novice learners to understand how individual learning areas facilitate their future work, how they relate to other learning areas and also acts as tool for problem reasoning in their early professional development.

Table 7.7 Phase 2: Hierarchical knowledge concept category table

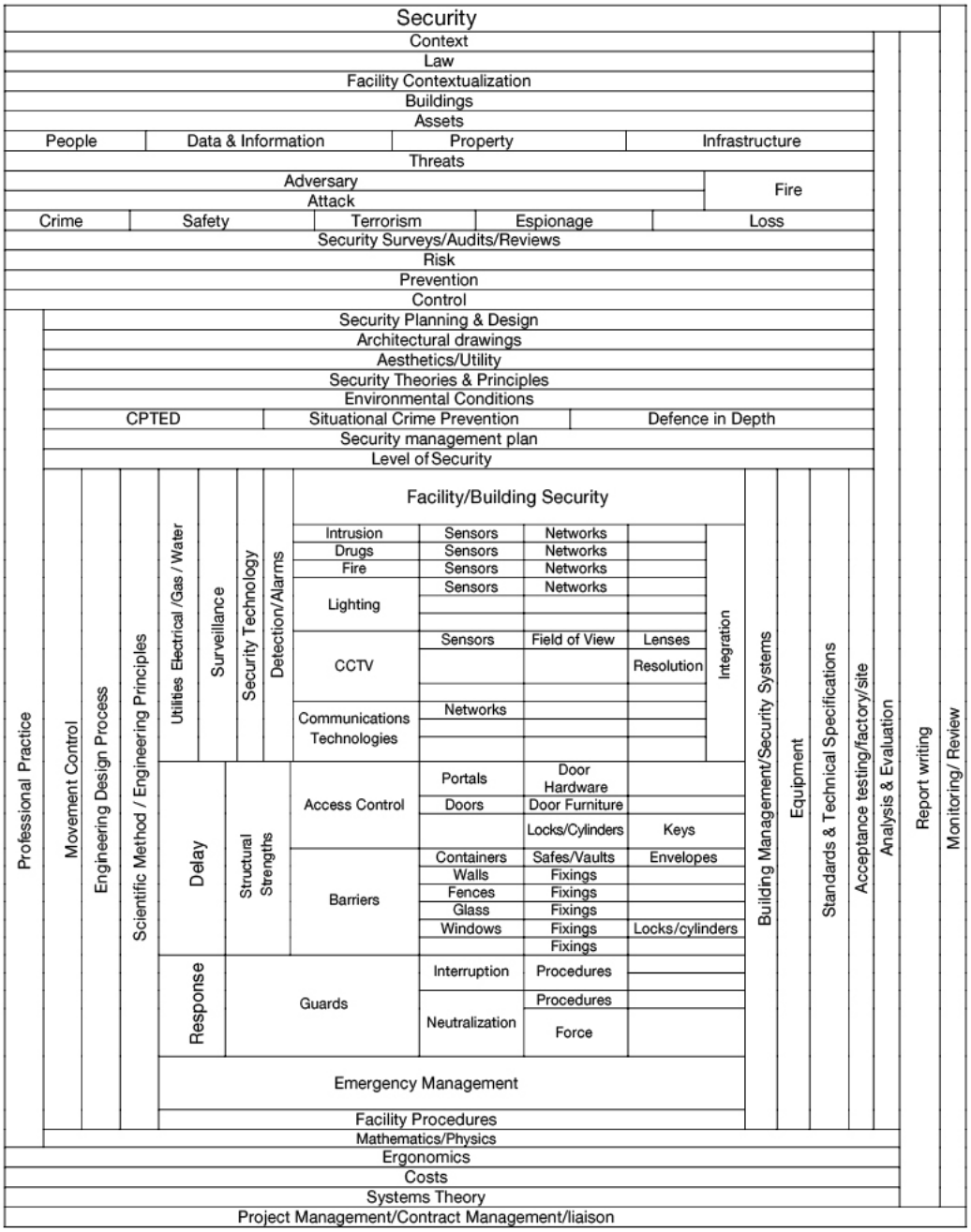
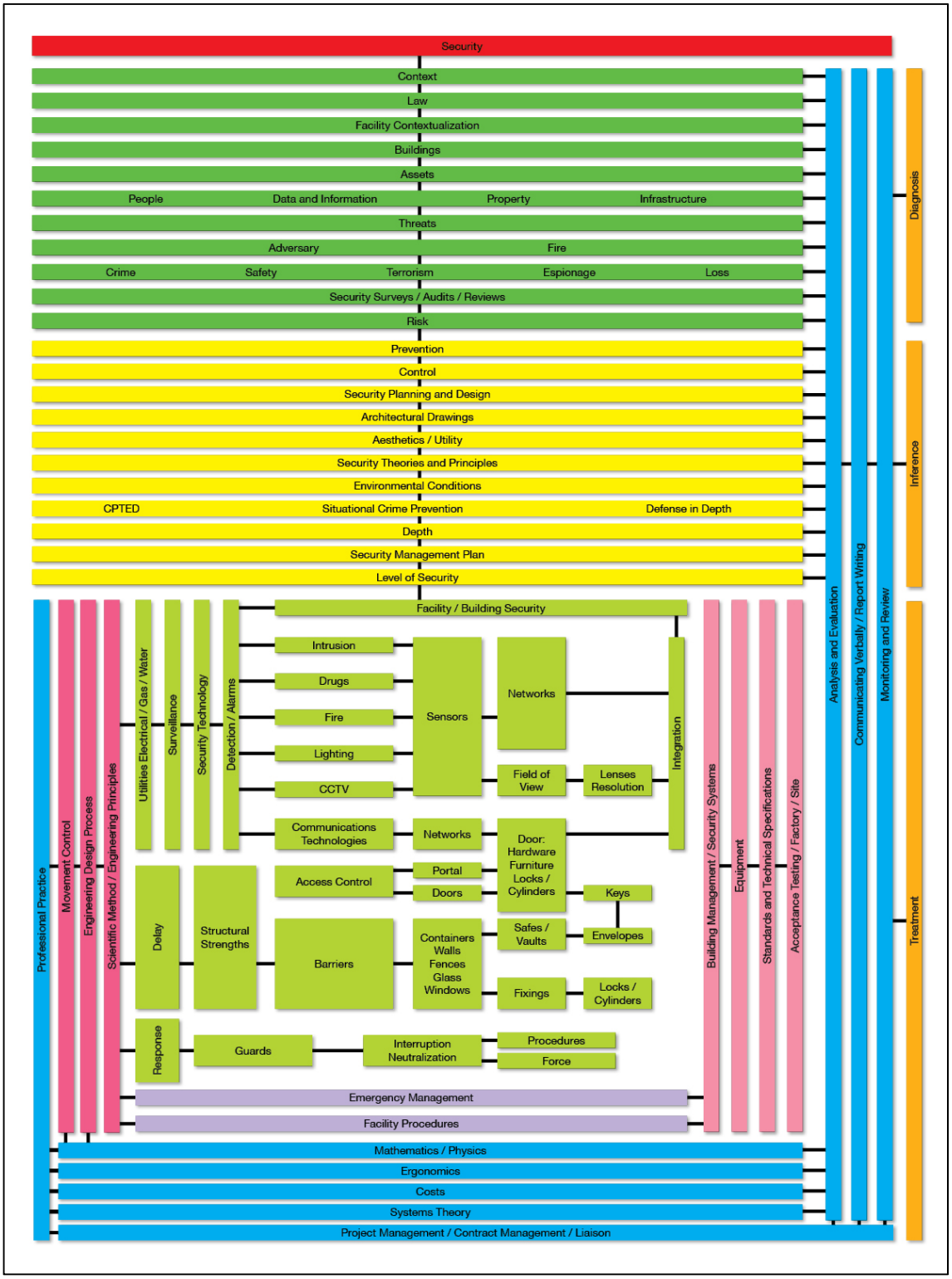


Figure 7.4 Physical security knowledge structure heuristic



7.5 Phase Two: Interpretation

Findings suggest that a broad and complex system of knowledge, or body of knowledge, (Table 7.6 and Figure 7.4) exists for physical security professionals. This knowledge basis includes as a minimum 98 knowledge areas which are required to be held by physical security professionals to be able to practice at a professional level. Thus reflecting back on the work of Abbott, professionals are premised to hold abstract bodies of knowledge that are not applied in a routine fashion, but require revised application, case by case (p. 7). Thus, Tables 7.6 present, as an iteration, such an abstract knowledge system. Within these tables each knowledge category has its own supporting body of literature that is applied by the professional or his delegate on a case-by-case basis. In addition, using Table 6.19 participants guided the integration of knowledge categories into the existing hierarchical Table (Table 6.19) to produce a new iteration hierarchical Table (Table 7.7) and cultural knowledge structure (Figure 7.4).

An analysis of Figure 7.4, based on the reviewed literature and pilot study findings, considers that, consistent with the three principles of professional practice (Diagnosis, Inference & Treatment) (Sections 3.1 & 3.3), physical security's knowledge system is hierarchically ordered to facilitate the initial diagnosis of the security problem, then reason about it towards developing a cost efficient treatment system. For example, knowledge located at the top of Figure 7.4 is specifically focused towards diagnosing the security problem. Consistent with Section 2.2, the knowledge structure commences with the very notion of security being pursued where diagnosis ends in risk articulation. Then professional inference or reasoning is engaged to articulate a desired level of real and perceived control to achieve security within the risk context. Such undertaking commences at prevention and finalises once the desired level is expressed. From this point the development of the security management system or physical protection system (PPS) becomes an engineering design and implementation task. At this stage, technical, physical and procedural elements are integrated to achieve contextually effective, yet proportional PPS as a risk treatment system.

Figure 7.4 demonstrates that such a knowledge structure comprises discreet sets of professional tasks, each with its own knowledge and procedures. However, these task

sets have a degree of inter-relatedness which stems from the premises and principles of the underpinning systems theory. This shared paradigm, represents what Fraser (1993, p.25) refers to as a body of knowledge. Also demonstrated in Figure 7.4 is a clear hierarchy within this body of knowledge where knowledge moves from a broader overview down to individual areas of occupational experts.

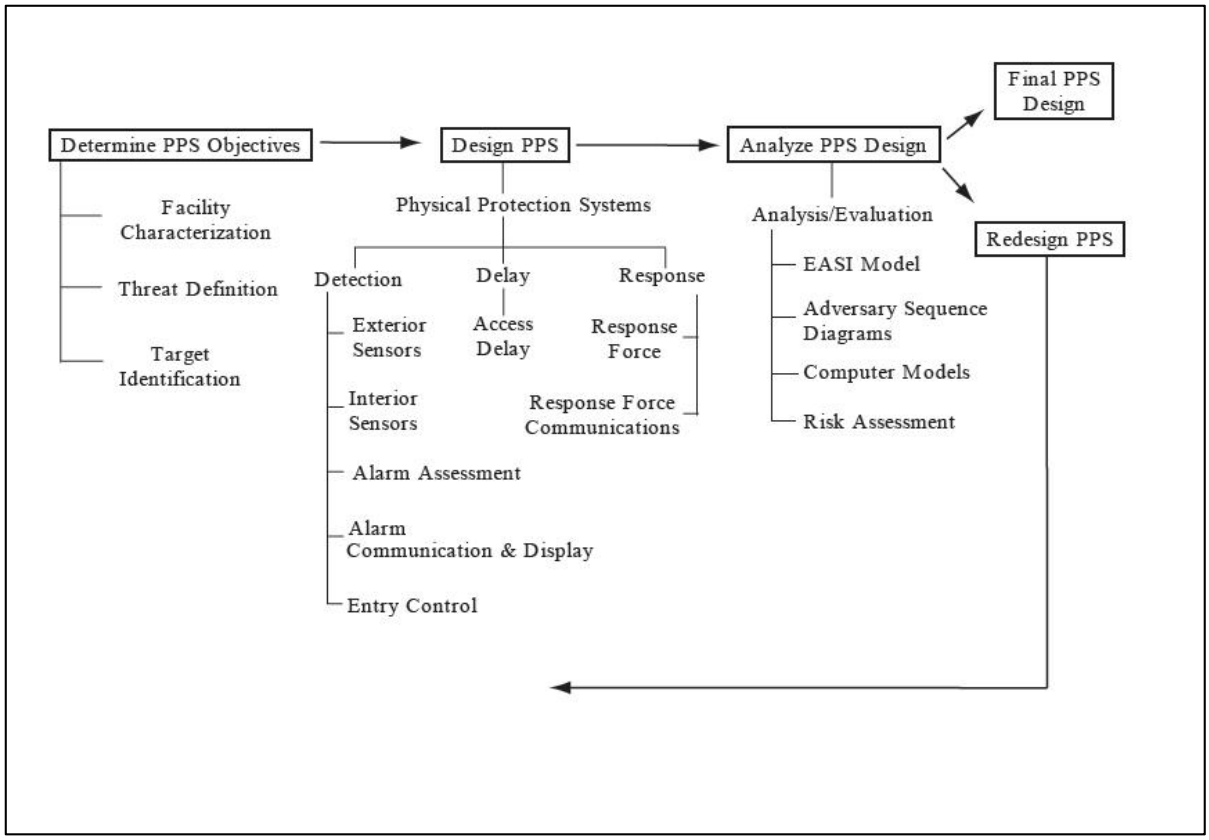
In principle such structural segregation of knowledge is supported through a percentage analysis of the first three salient physical security texts reviewed for Phase One of the study (Section 6.2.1). Text one was The Design and Evaluation of Physical Protection Systems where content percentage analysis indicates that knowledge to diagnose the security problem represents 21% of the text's information. In contrast, 79% of the text's contents are focused towards engineering treatment knowledge. Text two was the Protection of Assets, where a content percentage analysis saw 20% of its information focused on diagnoses of the security problem and 76% of its works towards more technical or engineering knowledge required to treat. Similar findings was also found for text three, Effective Physical Security where 25% of the information is focused towards diagnosing or reasoning about the security problem, whereas 75% is focused towards more engineering or technical treatment category knowledge. Moreover, all texts' information was hierarchically organised from diagnosing and reasoning (inferring) about the security concern, to technical knowledge for understanding how to treat the problem.

Furthermore, this structure is also arguably supported within Garcia's (2008) physical security planning heuristic (Figure 7.5). In her text, Garcia (2008, p. 3) explains that an effective PPS design commences with gathering information about the facility to be protected, its operations, conditions, operating states and defined threat. This forms a risk profile of the facility which steers the objectives of the PPS, as now the designer knows what to protect from whom. The next step is then explained as articulating the design for the new system, or re-design for an existing system, emphasizing that each facility is unique, so the process should be followed each time there is a need. Thus, once the risks are established the next step is to determine how best to combine the functional security elements to mitigate the threats which pose a risk such as fences, sensors, procedures, communications and so on. It is at this stage in the process that

professional inference is drawn on, utilizing a security design framework or philosophy to articulate a strategy and level of security.

Treatment is then more consistent with the engineering design process to articulate a design solution. Once the PPS is designed, Garcia expresses that an analysis and evaluation of the proposed PPS is conducted and where necessary a re-design undertaken. According to Garcia (2008, p. 9) without a methodical, defined analytical assessment, the PPS might waste valuable resources, provide unnecessary protection, or worse, fail to provide the adequate protection. This process is emphasised in her design heuristic (p. 15) (Figure 7.5) which indicates the relationship between risk and engineering design methodology utilized to achieve an effective PPS. The knowledge Table (Table 7.7) and heuristic (Figure 7.4) are congruent with Garcia's works. However, from an andragogical standpoint, they highlight in detail the occupational knowledge required to arrive at the commissioned solution.

Figure 7.5 Garcia's (2008) PPS design and evaluation heuristic



The physical security knowledge heuristic is supported by broader knowledge and skills that facilitate such a professional undertaking. Such skills include communication skills, or the ability to critically analyse and evaluate information and then communicate this to all stakeholders in a project. Figure 7.4 indicates that educationally some knowledge is taught to students for the purposes of professional diagnosis, some towards establishing proportional control or influence (inference), while other more technical knowledge is engineering based, towards the design and development of the appropriate PPS. This is supported by general graduate level occupational skills that facilitate professional practice.

Throughout this phase of the study there was an emphasis on the need for communication skills, engineering process and fundamentally that students of physical security must learn and understand the sciences (mathematics & physics) that underpin the treatment components and the principles of systems thinking that integrate individual elements into the barrier system. Students must also be formally schooled in the professional skills that facilitate professional practice, such as the ability to critically analyse data, to communicate clearly and effectively their analysis, to communicate with other professionals, to plan and coordinate activities and problem solve along the way to ensure treatment systems are commissioned accordant with technical specifications. Finally, there was consensus among the security professionals that graduates not only require the knowledge requisites included within the tables, but also on the ground experience.

7.6 Phase Two: Reliability and trustworthiness

To enhance the trustworthiness of the data, all interviews were recorded and fully transcribed enabling close and repeated analysis of the data (Schensul, LeCompte, Nastasi & Borgatti, 1999). This provided step one in establishing trustworthiness and validity in Phase Two's outcomes. From this point further reliability of Phase two stems from the view that qualitative data itself is not what is questioned, but rather the inferences drawn from them (Maxwell, 1992, p. 283). For qualitative research Maxwell (1992, p. 284) explains that validity is not a sole product of any methodology, rather it pertains to the data accounts, or conclusions reached. Therefore, both descriptive and interpretative validity techniques were employed within Phase Two.

Descriptive validity was achieved utilizing a narrative account of what participants said, which along with the transcripts provided trustworthiness; where the narrative supported by the transcripts provides such validity. Descriptive validity was supported by interpretative validity, using participant's own language, relying as much as possible on participant's own words and concepts (Maxwell, 1992, p. 289). Then, where possible, knowledge categories provided by participants were validated through knowledge categories derived from textbooks thus, providing a degree of triangulation in the data (Creswell & Miller, 200, p. 126). In addition, consistent with Phase One's reliability and validity, where possible outcomes were taken to other participants within the phase providing a degree of verification through member checking (Creswell & Miller, 2000).

7.7 Phase limitations

Phase Two of the study did experience a number of research limitations that influenced the findings which must be acknowledged. These include:

- Variations in security language, or rather variations in how terms are used to express meaning. Security does not have a domain discipline dictionary of agreed terms. Language variations in the security domain have been recognized by Manunta (1999) and these cannot be ignored as potential comprehension biases in forming knowledge categories. The pilot study sought to provide priori categories through synonymous term merging and clarity but not all knowledge categories could be subjected a detailed language analysis;
- The population sample was small relative to the amount of practitioners working within the physical security and broader security advisory fields. However, the study sought a first iteration ideal knowledge system not a perfect one, where Rundblad's (2006) work highlighted that for such qualitative research few participants are required (Section 4.3.1);
- Interviews were limited in time as participants interviewed could only spare around one hour for the interview process. Therefore this time frame restricted the depth of knowledge that could be generated in this Phase;

- The deductive analysis of category relationships based on the work of Spradley (Section 4.3) to form Tables 7.7 and Figure 7.5 was also a limitation within the study. This produced a qualitative analysis of relationships based on similarity and dissimilarity rather than a statistical analysis of a larger population sample. While participants were used to check the researcher's analysis to overcome relationship concerns, participants brought their own biases to this aspect of the study; and
- This phase also highlighted some variation in location of core and subordinate concept, as John stated, "not all relations between concept categories will be linear". Again, such limitations influence the outcomes of Phase findings.

7.8 Conclusion

This chapter presented the methodological process (Section 7.2) and interview analysis (7.3) towards the articulation of a system of knowledge for physical security professionals. Section 7.4 presented the findings for Phase Two. Phase Two upheld the principles of constructivism, showing that knowledge is constructed based on previous knowledge (Novak, 1993, p. 167). For instance, Table 7.7 and Figure 7.4 support the proposition that knowledge is constructed (Section 1.8), based on the foundations of previous knowledge (Tables 6.17, 6.19 & 7.5) and that this applies to the cultural domain of physical security. This phase found that cultural knowledge for the domain of physical security can be constructed and that consistent with Fosnot's (2005, pp. 27-28) work, such cultural knowledge is a whole larger than the sum of its individual cognitions; it has a structure of its own. Table 7.5 and Figure 7.2 uphold this view.

Section 7.5 presented Phase Two's interpretation explaining that for higher education Table 7.7 and Figure 7.4 highlight that novice students in the physical security domain require hierarchically the knowledge and its facilitated skills to diagnose the security problem. This includes as a minimum 98 knowledge areas, each with its own supporting body of literature that must be held by physical security professionals to be able to practice at a professional level. This requires the scientific process or method of considering the contextual threats, engaging in a level of analysis to articulate an accurate as possible depiction of the risks, then communicating this risk effectively so that a level of security can be set to overcome the problem. This phase also showed that students of physical security also require fundamental knowledge of the relevant

security theories and principles that enable them, based on the risk context, to develop a management plan that effectively mitigates the risk accordant with the economic law of diminishing returns (Section 2.2). Phase Two's reliability and trustworthiness was discussed in Section 7.6, followed by phase limitations in Section 7.7.

Chapter 8: Study Phase Three: MDS knowledge description

8.1 Introduction

This chapter presents Phase Three of the study, the quantitative mapping of physical security's macro knowledge structure to depict broader relationships between concept categories. The chapter commences with concept category reduction, as it was not feasible to measure all physical security concept proximities due to the length required for a multidimensional statistical scaling (MDS) questionnaire. The chapter therefore begins with Section 8.2, explaining knowledge concept category reduction rationale.

The MDS survey questionnaire was divided into two separate questionnaires to increase participation and reduce withdrawal rates. Section 8.3 of the chapter presents the survey's research findings, such as cluster and dimensional analysis of the MDS graphical maps. The findings are interpreted in Section 8.4, where a response to this phase's research question is presented. Section 8.5 discusses the reliability and validity for this phase of the study; however, its limitations are acknowledged in Section 8.6. The chapter concludes in Section 8.7.

8.2 MDS knowledge concept category reduction

The findings from Phase Two uncovered a broad range of knowledge category concepts and their supporting elements, together with their localised structure to form a new iteration physical security knowledge system. Phase Two's structure was developed using a qualitative ethnographic analysis technique accordant with the work of Spradley (1979). This technique produced Table 7.7 and Figure 7.4, which highlight a large number of superordinate or subordinate knowledge concept categories and their structure (N=98) within the cultural domain of physical security. Nevertheless, as John stated in his interview, "not all elements will be linear and locating some of the relations is very difficult as all persons bring a different experience to the study". This individualised bias could only be overcome through a psychometric map providing a group summation of concept locality, achieved using a multidimensional statistical survey questionnaire.

However, when developing the multidimensional statistical scaling (MDS) questionnaire there was an inability to take forward and map all 98 knowledge

categories. As established in the methodology (Chapter 4), such an approach would result in a survey questionnaire beyond achievable limits. Therefore, the completion of this phase required concept reduction to reduce the 98 knowledge categories and subordinate content areas (Table 7.6) to a more measurable 24. The notion of superordinate and subordinate knowledge categories, as depicted in Table 7.7 and Figure 7.4, facilitated a level of concept reduction to develop the survey questionnaire. Using this approach lower-order, more operational, subordinate categories were excluded for later mapping in separate studies. The aim of this phase of the study was to establish the broader content areas and their macro level structural organization rather than to map the concentrated operational connections within each category content area.

Concept reduction was deductively achieved through a superordinate and subordinate relationships analysis accordant with the professional tasks of diagnosis, inference and treatment. This approach saw subordinate content excluded that was more representative of lower strata processes undertaken by professionals or occupational tasks within the physical security knowledge system (Figure 1.1 & Figure 3.3). For instance, the top section of Table 7.7 saw the retaining of the cover term security, subsuming the underpinning yet lower principles of prevention and control as these were considered subordinate to and embodied within the broader cover term security (See Section 2.1). Context was another superordinate category taken forward into Phase Three, as Table 7.7 highlighted it as superordinate to law, facility contextualization and buildings, as the context is something that must be established prior to more focused analysis. As Bruce stated in the pilot study (Chapter 5), context is extremely important, it must be established before anything else. This very point was also emphasized in Section 2.2.1 of the reviewed literature, where drawing on the work of Baldwin (1997, p. 8) concept definition embedded into contextualisation facilitates tailored attainment.

Threat was also displayed as a salient diagnosis category in Table 7.7, as consistent with the reviewed literature (Section 2.2.1) security's foci is towards managing malicious centred human acts, articulated as threats rooted in conceptions of risk. As Manunta (1999) said, if there are no threats there is no risk, and security's roles have been articulated to manage the threats which pose a risk. Therefore threats was considered superordinate to categories including risk, adversary, attack and its embodying contexts

including crime, safety, terrorism, espionage, loss and fire and therefore taken forward as a prominent concept category. In addition, buildings was considered subordinate to facility contextualization which was subordinate to context and thus not taken forward as an individual category. This review resulted in a reduced list of knowledge categories more associated with the professional task of diagnosing the security problem (See Section 3.3). The deductive analysis procedure led to the development of Table 8.1, the superordinate diagnosis knowledge concept categories for physical security professionals.

Table 8.1 Physical security's superordinate diagnosis knowledge categories

Diagnosis knowledge categories		
Security	Threat	Context

Consistent with Section 3.3 of the reviewed literature and the findings of the pilot study (Chapter 5) the next professional practice task was inference or reasoning about the problem. As such, a number of categories were taken forward into Phase Three based on their prominent focus towards reasoning about the treatment of the security problem. This included security planning and design, because it was considered superordinate to aesthetics, utility, architectural plans and security theories and principles. In addition, the category of environmental conditions was one which required specific additional professional knowledge and was therefore also carried forward. Furthermore, specific security theoretical approaches were also considered core knowledge in the inference process and therefore carried forward into Phase Three's analysis. These categories included CPTED, situational crime prevention and defence in depth. Combined these approaches aimed to develop a security management plan that ultimately set a desired level of control or influence accordant with the risk context. This analysis led to the development of Table 8.2, physical security's superordinate inference process knowledge categories.

Table 8.2 Physical security's inference focused knowledge categories

Inference knowledge categories		
Security planning & design	Environmental conditions	CPTED
Defence in depth	Situational crime prevention	

Following inference, the final professional practice task is considered problem treatment. Therefore a number of knowledge category areas were taken forward into Phase Three accordant with their prominence as treatment categories. For instance, movement control was displayed in Table 7.7 as a salient treatment concept, superordinate to the lower strata category of access control. Surveillance as a concept was also considered a superordinate treatment category, as was detection, albeit, subordinate to surveillance. Technology as a prominent category was also taken forward into Phase Three. Supporting surveillance and detection were the prominent categories of sensors, lighting and CCTV, which have been highlighted as major areas of knowledge for contemporary physical security professionals.

Delay was another superordinate concept category embodying a number of subordinate yet essential knowledge areas. This knowledge area also included the broader categories of barriers along with an understanding of structural strengths as underpinning elements in achieving contextual delay. Barriers supported by structural strengths were considered superordinate categories embodying the subordinate categories of walls, glass, windows and fences. Security containers was emphasised by Brian to be a discrete knowledge area that was superordinate to categories of containers such as safes and vaults and security envelopes. Locks and cylinders was also carried forward as a significant category. Furthermore, response was another superordinate concept category in achieving effective security. This prominent category included the subordinate categories of guards, interruption, neutralization, procedures and force. This analysis saw the development of Table 8.3 highlighting physical security's treatment focused knowledge categories.

Table 8.3 Physical security's treatment focused knowledge categories

Treatment knowledge categories		
Movement control	Surveillance	Detection
Technology	Lighting	Sensors
CCTV	Delay	Structural strengths
Barriers	Security containers	Locks/cylinders
Response		

The deductive analysis also highlighted a number of knowledge category areas which provide knowledge and skills that facilitate professional security practice. For instance, professional practice was considered superordinate to the categories of project management, communications and report writing. Analysis and evaluation was also considered a prominent professional enabling category. This was pointed out in the pilot study by Frazer (Section 5.3.1.1), the ability to critically analyse and evaluate information in professional practice of diagnosing, reasoning about and treating security problems is considered essential. Finally, engineering design process, superordinate to engineering principles and scientific method was also considered an essential professional enabling category. This concept reduction analysis led to the development of Table 8.4, physical security's professional enabling categories.

Table 8.4 Physical security's professional enabling knowledge categories

Professional enabling knowledge categories		
Professional practice	Engineering Design process	Analysis & evaluation

Combined the hierarchical table (Table 7.7) facilitated the extraction of prominent knowledge areas for diagnosing the security risk concern, inferring about it for design purposes, and the design and commissioning (treatment) of a suitable protection system braced by professional enabling knowledge areas. The concept reduction analysis saw the development of Tables 8.1, 8.2, 8.3 and 8.4. In support, concept reduction knowledge categories were tested for reliability using Cronbach's alpha. Cronbach's alpha is a test of internal consistency assessing the extent to which questions within a questionnaire tapping a single underlying construct (physical security) covary (Allen & Bennett, 2012, p. 211). Cronbach's Alpha produced a high reliability value ($\alpha = .913$) indicating a strong relationship between knowledge concept categories from Tables 8.1.

8.2, 8.3 and 8.4 and physical security. Such analysis led to the final development of Table 8.5, Phase Three's 24 prominent physical security knowledge concept categories to be subjected to an MDS survey questionnaire analysis.

Table 8.5 Phase Three: Superordinate knowledge categories

Phase Three salient physical security knowledge categories		
Security	Threat	Context
Security planning & design	Environmental conditions	CPTED
Defence in depth	Movement control	Surveillance
Detection	Technology	Lighting
Sensors	CCTV	Delay
Structural strength	Barriers	Security containers
Locks/cylinders	Response	Professional practice
Engineering design process	Analysis & evaluation	Situational crime prevention

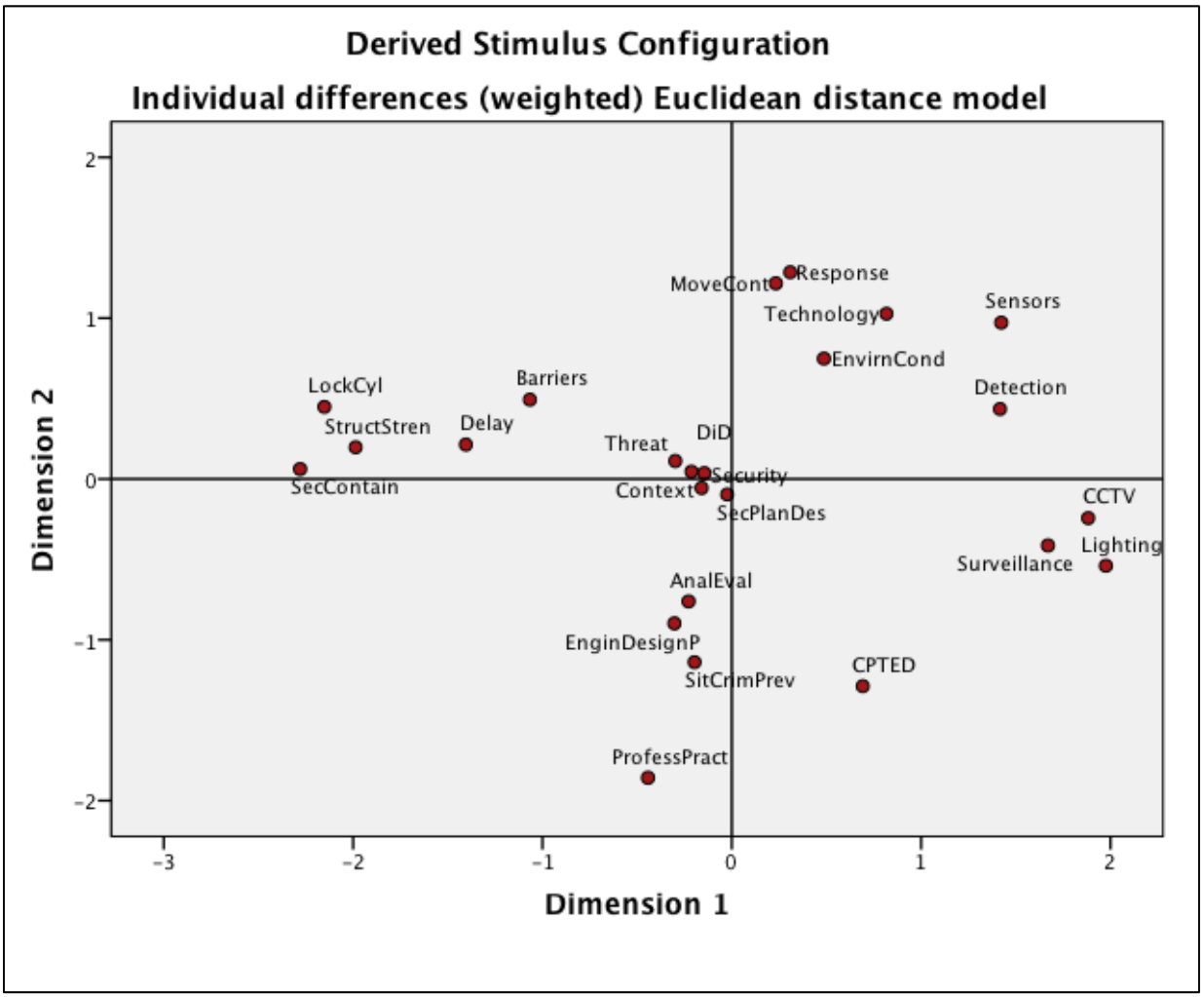
8.3 Findings MDS survey questionnaire

The MDS survey instrument (Appendix E) embedded Table 8.5's prominent knowledge concept categories and subordinate content areas into a survey questionnaire for paired comparisons to uncover global knowledge structure for the domain of physical security. Phase Three sought to respond to the question: What is physical security's macro knowledge content structure? MDS enabled a response to this question based on aggregated perceptions of dissimilarity amongst physical security concepts. The survey was preceded by a set of instructions providing a summary overview of the study and survey completion instructions. Concepts were rated by participants according to their perceived dissimilarity on a ten point rating scale, where ten indicates they are highly dissimilar and therefore further apart, and one indicated they are very similar or highly related and therefore extremely closer together. These measures were then averaged (mean) and standard deviations examined as a method for understanding shared (group) perceptions.

Figure 8.1 presents the MDS two-dimensional spatial map analysis produced using SPSS. This map is accordant with the writings of Davies and Coxon (1982, p. 6) who express the need for a spatial solution of three or preferably less dimensions so that the structure of the entire configuration can be visually interpreted. This view was shared by

Shepard (1972, p. 4) who pointed out that finding interpretable axes becomes considerably more difficult and uncertain when the number of dimensions exceeds what can be immediately comprehended in a picture or model. The initial MDS ALSCAL analysis produced Figure 8.1 highlighting macro spatial representation of physical security concepts.

Figure 8.1 Phase Three: MDS spatial representation of physical security concepts



The interpretation of the MDS map requires a key (Table 8.6), relating mapped concepts to those presented in Table 8.5.

Table 8.6 MDS survey key

MDS Key		
Security = Security	Threat = Threat	Context = Context
SecPlanDes = Security Planning & Design	EnvirnCond = Environmental conditions	CPTED = CPTED
DiD = Defence in depth	MoveCont = Movement control	Surveillance = Surveillance
Detection = Detection	Technology = Technology	Lighting = Lighting
Sensors = Sensors	CCTV = CCTV	Delay = Delay
StructStren = Structural strength	Barriers = Barriers	SecContain = Security containers
LockCyl = Locks/cylinders	Response = Response	ProfessPract = Professional practice
EnginDesignP = Engineering design process	AnalEval = Analysis & evaluation	SitCrimPrev = Situational crime prevention

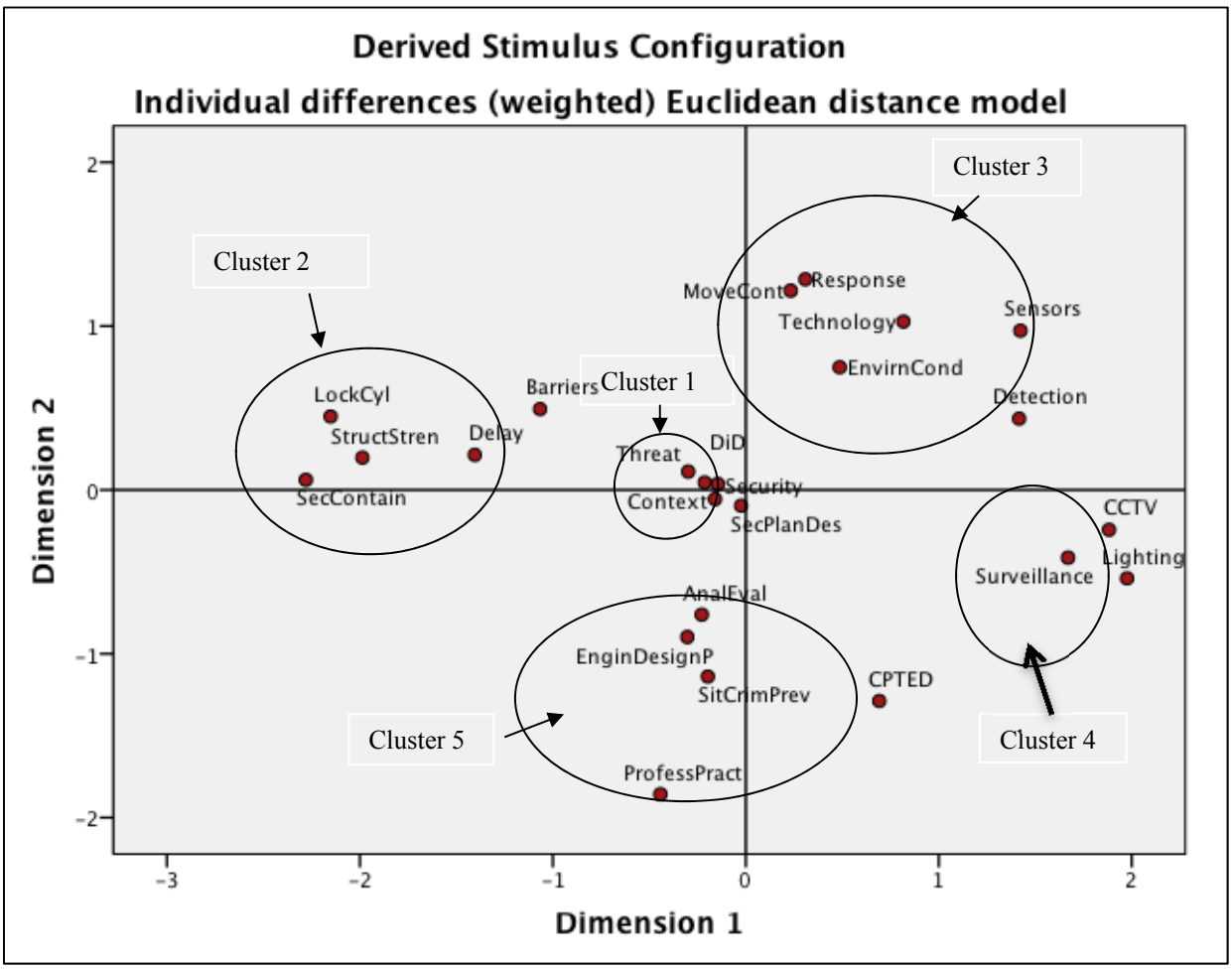
Nonetheless, a further analysis of the MDS output analysis was undertaken, specifically in relation to concept locality and their relations to other concepts (Figure 8.2).

8.3.1 MDS cluster analysis

The MDS map captured global structure by locating each concept in an N-dimensional space accordant with proximity correlations. For Figure 8.1 the calculated distances between concept points represent participant's averaged psychological proximity of physical security's knowledge concepts. The analysis undertaken was based on the work of Davies and Coxon (1982, p. 6) who emphasized that for interpreting such an MDS solution, clusters and dimensionality, including circular and linear orderings, need to be explored. Therefore MDS provided for two modes of interpretation, primarily clustering of concepts based on their close or distal proximity identified as Clusters1 to 5 (Figure 8.2) and their dimensional locality (Figure 8.3) according to their cultural separation.

For Phase Three, primary interpretation was achieved through a cluster analysis, as Brooks acknowledged and McAleese (1999) expressed, experts cluster together similar concepts, and separate unlike concepts, therefore clustering of like concepts should produce what McAleese termed "knowledge arenas".

Figure 8.2 MDS physical security knowledge clusters



8.3.1.1 Cluster One: Security

Central to the MDS spatial map was the cover term security, representing the desired state to be functionally achieved from the body of knowledge. Security, as the innermost category within the MDS spatial map, is consistent with the premises of a cultural domain. A cultural domain's knowledge structure is based on isolating the fundamental units of knowledge accordant with a single semantic relationship with its cover term, and organized according to relationships in terms of similarity and differences (Section 1.5). The central position of security is consistent with this premise and further supports the overarching seating of security for Table 7.7 and Figure 7.4. Clustered with security was the theory of defence in depth, an influential theory used to achieve an effective state of security with a distal mean of 1.4 and a standard deviation of 0.74, indicating participants collectively perceived these two concepts as highly

similar. Also closely correlated to security was threat as the driver or reason for security with a mean of 1.94 and a standard deviation of 1.00, again reflecting a high degree of consensus across participants for these associations. The position of threat within the spatial map was consistent with its MDS spatial position in Brook's 2008 study.

The next associated relationship within Cluster One was security and context, representing the concept used for understanding the specific security problem with a distal mean of 2.13 and a standard deviation of 1.41. Again, indicating consistent perceptions of correlation. Security planning and design as the means of reasoning about the security for a built environment was also clustered with the notion of security, with a mean of 2.33 and a standard deviation of 1.35 reflecting consensus perceptions amongst the sample. Cluster One saw knowledge requisites from the top section of Figure 7.4 centrally clustered together, in primary supporting the upper structure of Figure 7.4, physical security's knowledge heuristic.

8.3.1.2 Cluster Two: Delay

Cluster Two saw high similarity ratings for those physical security measures that aim to protect through their material strengths and design facets (Section 3.3) with concept categories reflecting delay or physical difficulty measures within physical security's knowledge base. Central within this cluster was the notion of structural strengths, and highly correlated with this was barriers with a distal mean of 1.79 indicating the concepts are highly similar, with a standard deviation of 1.12 indicating that all participants saw these concepts to be associated. Locks and cylinders were also highly similar to structural strengths with a mean of 2.0 and a standard deviation of 0.96. This measure of association reflects a strong consensus with this pairing. Delay was also highly correlated with structural strengths, with a mean of 2.21 and a standard deviation of 1.48; again reflecting a high degree of consensus across the sample for this relationship measure.

This cluster also included security containers as strongly associated to structural strengths, with a mean of 2.29 and standard deviation of 1.64, reflecting consistent perceptions across the sample for this pairing. Cluster Two saw knowledge concept categories from the delay aspect of Figure 7.4's treatment section grouped together, with MDS spatial localities consistent with local connection proximities. This again, in principle supports both the placement of, and local connections within Figure 7.4 and

indicates how cultural knowledge is associated with other cultural knowledge within the physical security sub-domain.

8.3.1.3 Cluster Three: Technology

Cluster Three included the concepts of technology, environmental conditions, movement control, sensors, detection and response. With the exception of response, within this cluster concepts are related to the issues influencing technology in the protection of assets which is supported by the literature. For example Garcia (2001, p. 173) expressed that entry control systems aim to achieve broader movement control of personnel and contraband into and out of a facility are nowadays technology based with the aim of detecting and delaying unauthorized movement. This point of view was also highlighted in the work of Walker (1988, p. 4 & 21). The inclusion of environment in this technology cluster may seem counter-intuitive however as Walker (1988, p. 21) notes, weather and other environmental factors have an impact on the efficacy of security technology, a point is also noted by Garcia (2001, p. 80).

Findings indicate that technology represents the pivotal category within this cluster. Technology and sensors reported a mean dissimilarity rating of 2.36. This association indicates these concepts are similar with a standard deviation of 1.22, suggesting general consensus. In addition, technology and detection were also closely correlated with a mean of 2.36 and standard deviation of 1.5, again indicating consensus with this pairing. Environmental conditions and technology were considered more distal; these concepts resulted in a dissimilarity mean of 3.17 and a standard deviation of 2.34, indicating broader perceptions of this pairing.

Technology and movement control presented a mean dissimilarity rating of 4.64 with a standard deviation of 1.78, and was located in close proximity to the delay treatment elements, indicating that participants felt that consistent with Figure 7.4 movement control, while technology based in contemporary times, is a broader security knowledge category representing a key security principle in the protection of assets. The final category within this group was response, with a mean rating of 5.5 and a standard deviation of 3.06, suggesting some divergence in perceptions of relationship with other technology focused elements. Response represented a single category from the human security categories and, on reflecting on other clusters, appeared difficult to locate in

relation to other categories. Perhaps with supporting elements it may have been better located.

8.3.1.4 Cluster Four: Surveillance

Cluster Four saw the grouping of those security knowledge categories associated with surveillance within a controlled or protected environment. Central within this cluster was the very notion of surveillance with technology based categories that help achieve a surveilled environment. For instance, surveillance and CCTV reported a mean dissimilarity rating of 2.29 with a standard deviation of 1.64, indicating that participants consistently saw these two categories as highly similar. Surveillance and lighting were also perceived as similar with a mean 2.71 and a standard deviation of 1.86. CPTED was also in the same quadrant, although separated from this tighter cluster. Nevertheless, due to the natural surveillance element within CPTED it reported a mean similarity rating with surveillance of 2.00 and a standard deviation of 1, indicating strong support for this association. However, CPTED was grouped with cluster 5 due to proximal locality and similarity with other inference related planning categories.

8.3.1.5 Cluster Five: Diagnosis, Inference and Treatment

Cluster five included analysis and evaluation, engineering design, professional practice and CPTED clustered around a central category of situational crime prevention. This cluster appeared to incorporate those knowledge categories more associated with understanding the security concern and treatment approach, or in the words of Abbott (1988, p. 40) to classify, reason, or - more formally infer - about the security problem. For instance, central within this cluster is situational crime prevention, a guiding theoretical framework for treating protective security problems. This cluster was located relatively closely to engineering design process, as a salient category in developing the treatment system, with a mean of 3.33 and a standard deviation of 2.3. Such spread indicates a reasonable consensus for this pairing. In addition, situational crime prevention and analysis and evaluation had a mean rating of 2.71 and a standard deviation of 1.64, indicating participants collectively felt these two categories were highly related.

CPTED – despite proximity to the surveillance cluster – was included with the diagnosis and treatment cluster due to its inherent planning aspects which influenced its

proximity with situational crime prevention, analysis and evaluation, professional practice and engineering design process. As Kerran stated, CPTED as a security/crime prevention theory is considered at the planning stage of the problem (Table 7.7), and includes natural access control, territoriality along with natural surveillance to mitigate security risk (Atlas, 2008). However the co-location of CPTED with surveillance is consistent with both Table 7.7 and Figure 7.4 along with earlier versions of the knowledge heuristic (Table 6. 19 & Figure 6.2) which saw CPTED proximally associated with access control and surveillance rather than with planning and design. This supports John's earlier statement that relationships will not always be linear.

Such complexity of relationships is also evidenced in the links between situational crime prevention and security planning and design as well as context which were not located within Cluster 5 but still within the same quadrant. Security planning and design recorded a mean rating of 2.53 and a standard deviation of 1.25 when compared to situational crime prevention indicating that participants perceived these to be closely related. Context (Cluster 1) and situational crime prevention (Cluster 5) were also considered highly related with a mean of 2.8 and a standard deviation of 1.93, indicating a strong degree of relationship.

This clustering also saw other relationships, for example, analysis and evaluation when compared to professional practice recorded a mean rating of 2.64 with a standard deviation of 1.45, indicating participants perceived these knowledge categories to be highly related.

An analysis of the clusters within the MDS space (Figure 8.2) indicates proximal relationships between concepts in N-dimensional space (Gonzalvo, Canas & Bajo, 1994). The clusters indicate concepts are spatially close or separated based on culturally perceived distances between all pairs of concepts (Gonzalvo, Canas & Bajo, 1994, p. 602). In addition, many of the cluster proximities between concept pairs support the localized structure presented in Figure 7.4 as a result of cultural connections from Table 7.7. Nevertheless, clusters on their own provide limited clarification of the domain's macro spatial relationships. As such, informed by the writings of Davies and Coxon (1982, p. 6) there is a need to search for spatial configuration-including dimensional orderings.

8.3.2 Dimensional interpretation

Dimensional analysis sought to understand the broader spatial relationships between individual concepts and clusters. Using this approach, the dimensions defining the space are premised to represent the main properties along which concepts within the domain are organized (Gonzalvo, Canas & Bajo, 1994, p. 601). Consistent with the pilot study analysis, dimensional interpretation focused on the salient dimensions of diagnosis and treatment. These are based on Abbott's (1988) identification of three salient tasks of the professional – diagnosis, inference and treatment, along with his view that inference is undertaken only when the connection between diagnosis and treatment is obscure or distal (p. 49).

Table 8.7 presents the calculated dimensional rating for each physical security concept and its relationship to the professional tasks of diagnosing a security problem or treating it. Higher scores indicate a greater degree of relatedness to a given dimension.

Table 8.7 MDS physical security dimensional data

Concept	**Diagnosis (Dimension 1)**	**Treatment (Dimension 2)**
Security	-.1597	-.0557
Threat	-.2985	.1120
Context	-.1454	.0359
SecPlanD	-.0246	-.0961
EnvirnCo	.4864	.7484
CPTED	.6914	-1.2884
DiD	-.2134	.0456
MoveCont	.2325	1.2165
Surveill	1.6694	-.4132
Detectio	1.4164	.4347
Technolo	.8169	1.0276
Lighting	1.9757	-.5399
Sensors	1.4228	.9720
CCTV	1.8823	-.2432
Delay	-1.4045	.2137
StructSt	-1.9866	.1970
Barriers	-1.0665	.4929
SecConta	-2.2802	.0620
LockCyl	-2.1519	.4484
Response	.3083	1.2854
ProfessP	-.4426	-1.8577
EnginDes	-.3031	-.8977
AnalEval	-.2283	-.7612
SitCrimP	-.1970	-1.1391

Figure 8.3 Physical security's knowledge structure in two-dimensional space

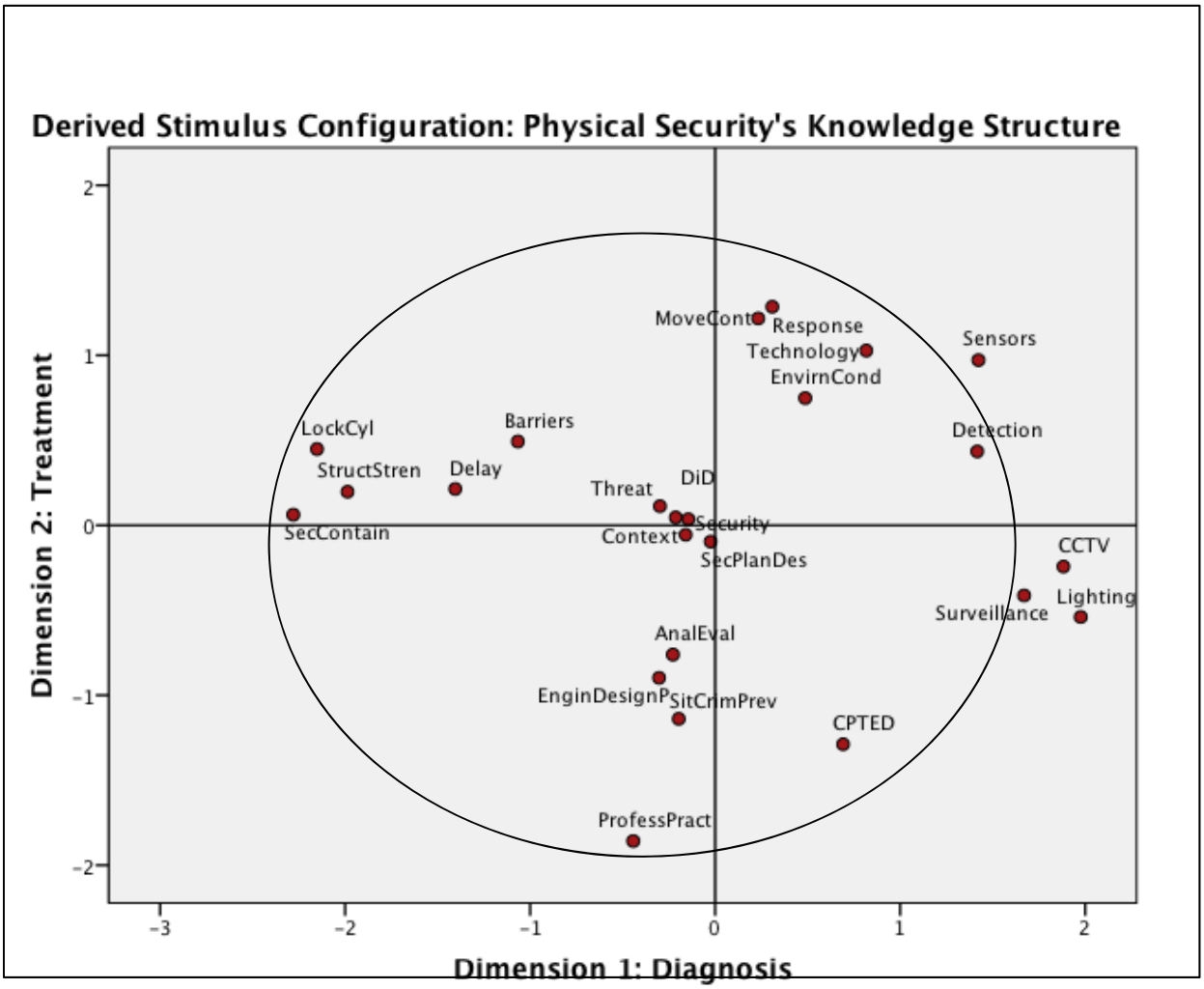


Figure 8.3 represents the SPSS output two-dimension MDS spatial map based on the values provided in Table 8.7.

8.3.2.1 Dimension Two- Treatment

For this analysis, physical security concepts most strongly related to the Treatment dimension were identified and listed in Table 8.8 ranked according to degree of relatedness.

Table 8.8 Treatment dimension

Dimension 2	
Response	1.2854
MoveCont	1.2165
Technolo	1.0276
Sensors	.9720
Barriers	.4929

Response was found to be the physical security concept most strongly related to treatment. This differs from the pilot study findings, but as Garcia (2001, p. 5) highlights, the primary functions of a physical protection system are the detection and delay of an adversary long enough to facilitate response by security personnel. Response according to Smith and Brooks (2013, p. 108) is the actual deployment of a system variable that either apprehends or drives away the adversary. Thus, the goal of the system is to provide enough time after detection, for a response element to take action (Garcia, 2001). This treatment category represents an essential means of securing an asset, as without response, detection and delay system variables are arguably inconsequential. Accordingly, this is an essential treatment option and its N-dimensional place along with its numerical rating as the highest treatment variable is arguably sound.

The second highest treatment category was that of movement control (MoveCont). This reflects the role of physical security being to prevent unauthorized access or egress (Garcia, 2001; Smith & Brooks, 2013, p. 105), which ultimately translates to controlling movement.

Technology was the third highest treatment category and in contemporary times, the use of technology in the protection of assets is standard practice and therefore a major knowledge area for the treatment of security concerns. According to Smith and Brooks (2013, p. 139) security technology associated with intrusion and access control and is concerned with the authorization, identification, and detection of people in circumstances that may provide a threat to an organization. Electronic security is a vital aspect of any security program (Pearson, 2007, p. Ix). According to Pearson enhanced sophisticated electronics is part of virtually every electronic security functional system (p. vii).

For a contemporary security professional to be effective they need to understand the electronics and the interactions of various electronic security functions to a high level, as they are integrated into a total security system solution (p. ix). Accordingly, sensors followed this category; these react to a stimulus and initiate an alarm (Garcia, 2001, p.

55), again a salient treatment element within any electronic security system (Smith & Brooks, 2013, p. 139). Barriers were also considered a salient treatment knowledge area for security professionals and as a category represent a pivotal means of treating security concerns, as Walker (1998, p. 19) states, the physical or fortress concept of protection has been with us from earliest times. Barriers provide the delay function of defence in depth to retard the progress of an adversary to provide the necessary time for an effective response (Garcia, 2008, pp. 60-61). Dimension Two straightforwardly related to those categories which afford physical treatment of protective security concerns.

8.3.2.2 Dimension One Diagnosis

For this analysis, physical security concepts most strongly related to the Diagnosis dimension were identified and listed in Table 8.9, ranked according to degree of relatedness. The concepts most related to diagnosis are lighting, CCTV, surveillance, sensors and detection.

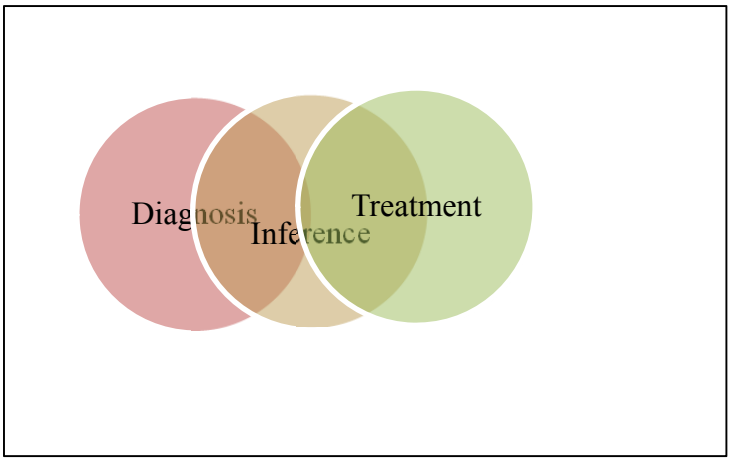
Table 8.9 Diagnosis dimension

Dimension 1	
Lighting	1.9757
CCTV	1.8823
Surveill	1.6694
Sensors	1.4228
Detection	1.4164

Further examination of Figure 8.3, the MDS spatial map visually representing the location of the physical security concepts across the dimensions of diagnosis and treatment, shows that some concepts rate highly across both dimensions. The work of Abbot can be drawn on to explain such an outcome. Abbott's (1988, p. 40) work conveys that in terms of diagnosis, inference and treatment, professionals often run these modalities together, stating the three are modalities of action more than aspects per se, and they relate to problem complexity (Section 3.3). According to Abbott, professionals vary their temporal structuring of diagnosis and treatment (p. 48) whereas in many cases the two coincide (diagnosis & treatment) (p. 45). Abbott states that where diagnosis is clear and treatment obvious, the path or time frame between the two is short, and formal inference omitted.

Furthermore, according to Abbott the professional may commence with treatment rather than diagnosis (p. 40), or may diagnose by treating, as doctors often do (p. 49). However, deeper professional reasoning (inference) is undertaken when the connection between diagnosis and treatment is obscure or distal (p. 49), and relates to, and draws on domain professional knowledge (p. 48) (Section 3.3). This means that security professionals may in fact see a number of knowledge categories as being associated with both diagnosing and treating the security problem. Abbott's (1988) views are expressed through Figure 8.4 which indicates the potential overlap for the modalities of diagnosis, inference and treatment of professional security problems and how this overlapping may obscure dimensional interpretation.

Figure 8.4 The overlap between diagnosis, inference and treatment of professional problems



In addition, for the practice domain of physical security, diagnosis represents a small subset of skills, where the majority of the technical knowledge is focused towards problem treatment and thus, such categories would logically dominate the two dimensional space. Dimensional interpretation for diagnosis was less conclusive than dimensional interpretation for treatment. Nevertheless, the dimensional space indicates how clusters of knowledge relate to other clusters of knowledge across the professional modalities of diagnosis and treatment and how due to the dual meaning of security terms knowledge concepts may be used to refer to diagnosing the problem and treating it.

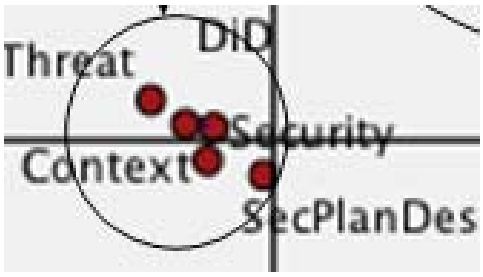
8.4 Phase Three: Interpretation

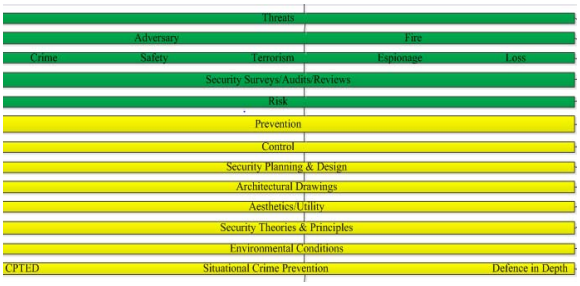
Phase Three of the study sought to respond to the research question:

What is physical security's knowledge content structure as measured by multidimensional statistical scaling?

Phase Three provided some valuable insights into the study's findings to date. For instance, a comparison between Figure 7.4 (Phase Two) and Figure 8.2 shows congruence with knowledge category organization. Figure 8.2 saw major knowledge concept categories clustered together at the top of Figure 7.4 for the professional tasks of diagnosis and inference. For example, Figure 8.5 shows that Cluster One in Figure 8.2 included the notion of security, the context in which security is being pursued, threats to security, security planning and design and defence in depth clustered together. These knowledge categories are also located together, although hierarchically at the top of Figure 7.4.

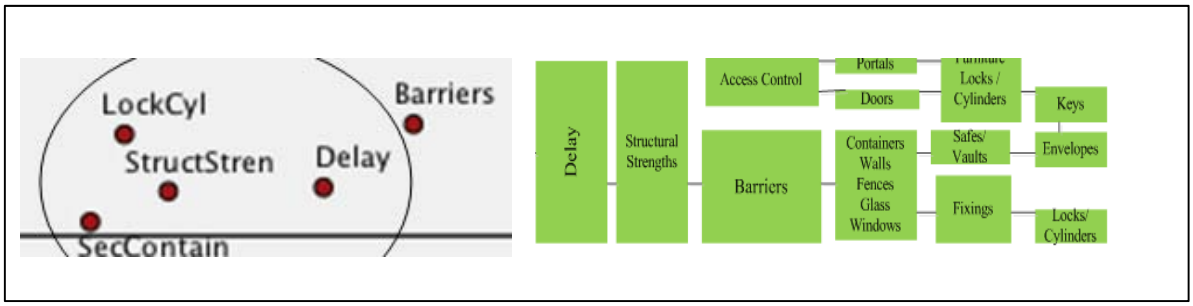
Figure 8.5 Comparison of diagnosis focused knowledge categories





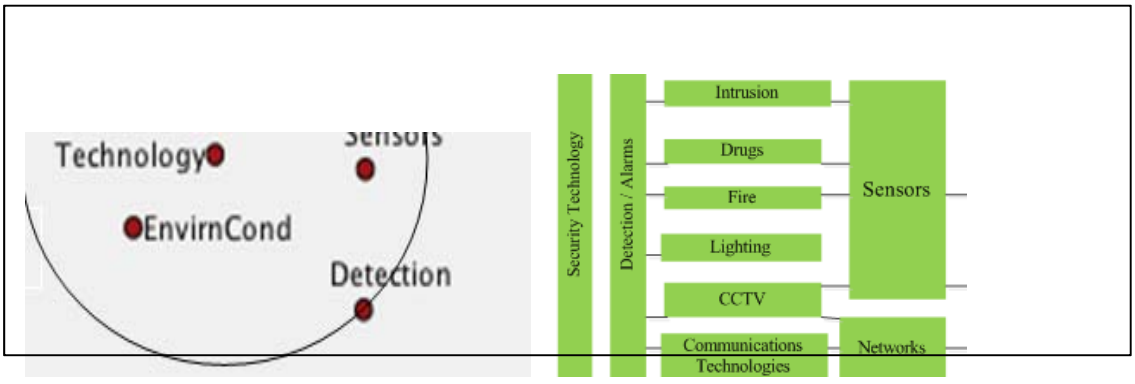
In addition, MDS Cluster Two (Figure 8.2) included major knowledge areas focused towards delaying an adversary's advancement. These included the concept categories of delay, structural strengths guiding the efficacy of delay, barriers, security containers and locks to functionally achieve delay. These knowledge categories form an engineering arm within the treatment section of Figure 7.4 (Figure 8.6), again showing consistency across the two knowledge models.

Figure 8.6 Comparison of delay focused knowledge categories



Furthermore, MDS Cluster Three (Figure 8.2) included movement control and response, overarching security goals which again both sit within the treatment section of Figure 7.4. However, it also located technical knowledge areas of elements employed to achieve security clustered together. These included technology, detection of the threat and sensors employed to detect the threats which pose a risk (Figure 8.7). Again, these knowledge categories form a technology arm within the treatment section of Figure 7.4. This group also included environmental conditions as these have a major influence in selecting security technologies and sensors for a context.

Figure 8.7 Comparison of technology focused detection knowledge categories



Cluster Four within Figure 8.2 saw three knowledge areas associated with surveillance or observation clustered tightly together. This included the concept of surveillance, supported by lighting and CCTV, the technical means to help achieve surveillance. In the same quadrant was also CPTED, as an element within CPTED aims to achieve natural surveillance (Atlas, 2008). Again, these knowledge areas clustered together also formed a logical surveillance arm within the treatment section of Figure 7.4 (Figure

8.8). In addition, the co-location of CPTED within this quadrant is supportive of CPTED's location within this section of Figure 6.2 (Phase One), supporting John's view that there will be knowledge overlaps.

Figure 8.8 Comparison of surveillance focused knowledge categories

Cluster Five saw the clustering of knowledge concept categories associated with facilitating professional practice. These included the categories of professional practice, engineering design process as well as analysis and evaluation. These are all knowledge concept categories which frame the treatment section of Figure 7.4; supporting the requirement for facilitating knowledge in the physical security professional's body of knowledge to achieve efficacious treatment. Interestingly, this cluster also saw situational crime prevention (SCP) within it; SCP is a major theoretical frame work for considering physical security and crime prevention within a defined context.

The clustering of knowledge (Figures 8.2 & 8.3) did support to a degree dimensional segregation according to diagnosis, inferring or reasoning and treatment as also depicted in Figure 7.4 showing local connections. This phase of the study saw a high degree of concordance between the taxonomy (Table 7.7), graphically presented in its supporting heuristic tool (Figure 7.4) and the MDS analysis (Figures 8.2 & 8.3). Such consistency provides validity towards the results for each phase of the study and facilitates a response to Phase Three's research question.

Phase Three's findings indicate that physical security's knowledge content structure relates to clusters of similar or related concept knowledge categories and subordinate concepts proximately organized in relation to the both the functional objectives the system aims to achieve, and the cognitive tasks required to realize the system's output functions. The cognitive tasks relate to knowledge categories focused towards diagnosis of contextual security or crime prevention problems and inferring about them to treat

them with suitable system variables. These problems relate to the manifestation of harm to people, information or property through malicious actors achieved through unlawful access or crime enablers (Section 3.3). For instance, Figures 8.2 and 8.3 highlights that the central concept is the notion of security, and clustered with this is the context being considered and the threats that poses a risk within that context. Such a cluster of concept knowledge guides the pursuit, and enables the achievement of a secure facility.

These concepts are highly related to security planning and design, which guides the evaluation and selection of treatment elements. Figures 8.2 and 8.3 support the structure of Table 7.7 and Figure 7.4 expressing the notion that physical security's body of knowledge is concentrated towards, and organized around diagnosing the security or crime concern, reasoning about it towards ascertaining the appropriate measures and levels of control, then planning and designing security strategies and practices that functionally achieve environmental control and therefore treat risk. As Abbott (1988, p. 44) states, treatment is organized around a classification system and a brokering process, where brokering gives results to the client. Phase Three provides a blue print (Figures 8.2 & 8.3) for establishing a knowledge or curriculum framework for future physical security professionals.

In terms of curriculum ordering principles, these figures indicate that physical security's knowledge content should be presented and taught in a manner that reflects physical security's professional tasks. These tasks include diagnosis, reasoning about (problem solving…inferring) then identifying, planning and designing and implementing treatment measures. For instance, the MDS spatial map indicated concept proximity for knowledge concepts relating to understanding the threats which pose a contextual risk driving the need for security (Cluster 1). It also indicated proximal relations for physical resistance treatment concepts (Cluster 2), electronic or technology based treatment options (Cluster 3), security surveillance elements (Cluster 4) and professional enabling knowledge and skill requisites (Cluster 5) that help produce the client's desired result. The structural similarity between Table 7.7 and Figure 7.4 (Phase Two) and Figures 8.1, 8.2 and 8.3 (Phase Three) support the validity of cultural domain mapping process as a means of expressing both knowledge requisites and structural relationships with other knowledge categories in the protection of assets. These figures show similarity in concept grouping according to hierarchical and linear relationships.

8.5 Reliability and Validity

As an analysis methodology MDS has the advantage of being low in experimenter contamination (Schiffman, Reynolds & Young, 1981, p. 30) and therefore results of the MDS analysis represent a reliable outcome. This was supported by the consistent spatial location of *threat* in Figures 8.1, 8.2 and 8.3 with Brook's 2008 MDS security risk management knowledge structure findings. Nevertheless, reliability was considered through a goodness-of-fit evaluation. This was evaluated according to Kruskal's Stress formula 1 and the Squared Correlations. The data analysis presented a Stress score of 0.24399 and an RSQ of .70566 (squared correlations in distances) indicative of reliable results for proximal interpretation. However, according to the MDS Stress measure, not all concepts were in their ideal spatial locality. Nonetheless, a stress score of 0.24399 is well within the 0.54 stress score tolerances argued by Rakshit and Ananthasuresh (2008, pp. 293-294). By using a graph of alternate dimensional settings and stress scores Rakshit and Ananthasuresh (2008, p. 293) were able to demonstrate that a stress score of 0.54 was acceptable for a valid MDS analysis, as it best fitted the correlational model; where both higher and lower dimensional increases in paired amino acid relations increased stress.

Thus, a two dimensional map with a stress score of 0.54 was the most appropriate means of visually presenting the hidden structure in Rakshit and Ananthasuresh's data set. This literature supports the view that a stress measure of 0.24399 was indicative of reliable results for proximal interpretation. Furthermore, validity was also tested against the MDS source data, using Cronbach's Alpha. This measures reliability through an alpha coefficient between 0 and 1. A measure of 0 for Cronbach's Alpha means that the source data are unreliable, whereas a measure of 1 represents perfectly reliable source data (Allen & Bennett, 2012, p. 211). Cronbach's Alpha produced a high (α=.913) value, indicating sound reliability and validity for the Phase Three survey questionnaire.

8.6 Phase Limitations

This phase of the study experienced a number of research limitations that influenced the findings, which must be acknowledged. These include:

As with previous phases, variations in security language, or rather variations in how terms are used to express meaning may have influenced participant's perceptions of how dissimilar and similar security concept categories were; and

The population sample was small relative to the amount of practitioners working within the physical security and broader security advisory fields. This phase of the study fell short of the desired MDS sample (N=30), analyzing 29 complete surveys. However, the analyzed surveys achieved 97% of the targeted sample producing a sound statistical outcome for matched dissimilarity and results indicated concordance with Phase Two pairings.

8.7 Conclusion

This chapter presented Phase Three of the study, the multidimensional statistical scaling analysis of prominent knowledge concept categories for the domain of physical security. The analysis sought to capture a psychometric map of knowledge structure for the cultural domain of physical security based on their similarity or dissimilarity to each other. Section 8.2 presented the first stage of achieving such an outcome, concept reduction of physical security categories. Then the Phase objective was achieved, using a proximity matrices questionnaire that asked participants to rate relations, or proximities, between content items from Table 8.5; where people judge the psychological distance or closeness of the stimulus to produce geographical representations. Section 8.3 presented findings from the MDS survey questionnaire, through Figures 8.1, 8.2 and 8.3; indicating how participants perceived the individual knowledge concept categories and subordinate concepts were considered to each other, uncovering macro cultural structure.

Section 8.4 presented the interpretation for this phase of the study, highlighting that physical security's knowledge content structure relates to clusters of similar or related concept knowledge categories and subordinate concepts or elements proximately organized in relation to the professional tasks of diagnosis of contextual security or crime prevention problems, inferring about them to treat them with suitable system variables. Phase findings indicate that physical security's knowledge content should be presented and taught in a manner that reflect the physical security professional tasks of diagnosis, inferring and treating physical security associated concerns. Nevertheless,

there were some limitations within the phase methodology and procedure which were presented in Section 8.6.

Chapter 9: Study Phase Four: Physical security knowledge evaluation

9.1 Introduction

This chapter presents Phase Four of the study, explaining what the knowledge concept categories and their cultural structure mean for the future of physical security education based on a focus group discussion extending on the findings from Study Phases Two and Three. Phase Four sought to understand what the knowledge requisites and supporting learning objectives are in terms of a desired curriculum for future physical security professionals. This phase also sought to explain how the knowledge requisites should be epistemically organised for adult learners, the depth and scope of the subject matter and the strengths and weaknesses in the knowledge heuristics for novice learners. Finally, this phase compared the body of knowledge as represented in the qualitative concept map (Figure 7.4) and MDS solutions (Figures 8.2 & 8.3) in relation to a desired curriculum framework through a discourse analysis.

The chapter is divided into a series of distinct sections presenting the sequential building of knowledge towards responding to the phase research question What are the knowledge requisites and supporting learning objectives for physical security professionals? Section 9.2 presents Phase Four's participants, highlighting the depth of physical security knowledge each member of the focus group brought to the study. Section 9.3 presents the focus group analysis, organised thematically according to what the experts revealed as the desirable curriculum attributes for future physical security professionals. Section 9.4 presents an interpretation of Phase Four's findings, responding to Phase Four's research question through a series of assertions brought forward from the pilot study. The Section 9.5 discusses the reliability and trustworthiness of Phase Four's findings and the chapter concludes with Section 9.6.

9.2 Participants

Phase Four incorporated a purposive sample of physical security experts (n= 7), including Clint, Peter, Frazer, Brian, Garrhett, Nicholas and Brad (Table 9.1). Based on the pilot study experience, each participant in Phase Four is actively practicing in an operational consulting capacity within the sub-domain of physical security. That is, each participant's occupational focus is saliently towards providing physical protection advice to clients due to their expertise in the sub-domain of physical security.

Combined, participants brought a rich depth of experience and thorough understanding of the professional knowledge requisites for graduates seeking entry into the physical security professional domain.

Table 9.1 Phase Four: Expert profiles

Name	Profile
Clint	A security and public safety consultant to public, local and state authorities. He also provides technical security and telecommunications training for security practitioners. Clint holds a Bachelor of Science (Security) and a Certificate III in Telecommunications.
Peter	Peter has over 25 years' experience providing protective security advice across a range of sectors including customs and border protection, the maritime domain, correctional and state infrastructure environments. Peter holds a Bachelor's Degree in Security Science, and a Diploma in Project Management.
Frazer	Provides protective security leadership, advice and management across numerous sectors both as a consultant and at a senior leadership level for companies and corporations. This includes mining operations, offshore oil and gas platforms, and government facilities both within Australia and overseas. Qualifications include a Bachelor of Science (Security), (Commas and IT), Certificate of Data Communications, Certificate of Organisational Behaviour and Management.
Brian	Qualified locksmith, security consultant, agent and installer, and lecturer in intrusion and access control systems. He brings 40 years of security expertise to the study, holding qualifications including Certificate III in Investigations, Certificate IV in Security and Risk Management, Certificate IV in Training and Assessment, a Diploma of Engineering Technology Security Engineering, and an Associate Degree in Training and Development.
Garrhett	A senior engineering security consultant, providing security related planning advice during the early stages of major projects. He worked as a science officer for the UK Home Office where he tested and evaluated security technology and is a sessional university lecturer.
Nicholas	A lecturer with the International Academy of Law Enforcement and Security Training group. He holds a Bachelor of Arts (Justice Studies), a Graduate Diploma in Education (Tertiary and Adult Education), a Graduate Certificate of Emergency Management, and is a Certified Protection Professional (CPP) and holds Port Facility Security Officer (PFSO) endorsements.
Brad	A security consultant for 21 years. With electronic technician qualifications he specialises in technology. Brad has worked on large capital works projects across the Middle East, Asia and Australia, and also runs an independent security technology test laboratory and associated infrastructure.

9.2.1 Administration of focus group

The focus group interview took approximately two hours, and comprised seven questions (Table 9.2) (Appendix F) to achieve the phase outcomes. The questions sought participants' thoughts relating to requisite knowledge, teaching structure and supporting learning objectives in response to previous phase findings, based on their

professional experience. It also sought their final opinion of the knowledge structure, and provided them the final opportunity to recommend adjustments to the hierarchical table and supporting heuristic. All experts were emailed the focus group questionnaire along with supporting figures and tables a week in advance, providing time for them to consider the objectives of the interview, questions and supporting tables and figures. The focus group was recorded and transcribed for later analysis (Appendix L).

Table 9.2 Phase Four: Expert focus group questions

No.	Interview questions
1	In terms of articulating a formal knowledge system, based on these maps, what do you see as the foundation knowledge unit requirements to be learned by physical security professionals before qualification?
2	Do you believe these maps capture the knowledge concepts required for a physical security professional, if not what do you consider is missing?
3	It is argued that higher education students should learn or know the science or knowledge on which their future domain is built. Based on this view, what is the depth of scope or focus for security higher education knowledge?
4	What should be learned after qualification, in professional practice?
5	Based on learning principles how should these knowledge units be organised?
6	What are the strengths and perhaps the weaknesses of these maps in terms of establishing a physical security professional's knowledge system?
7	Based on what has been discussed so far and the knowledge heuristics, what are the higher education learning objectives for future physical security professionals?

At the commencement of the focus group the study's jurisdictional objectives were contextualised to all participants. It was explained that the focus for the study was steered towards a graduate who, having completed a tertiary security program, was seeking to work in the physical security field; diagnosing security problems and designing and commissioning a system to mitigate these.

9.3 Focus group analysis

9.3.1 Physical security foundational unit requisites

Phase Four findings strongly support that both the qualitative knowledge heuristic (Figure 7.4) and the MDS analysis (Figures 8.2 & 8.3) capture the foundational knowledge requisites for graduate physical security professionals. Participants supported the requirement for all knowledge areas presented in Table 7.6 and Figures 7.3, 8.2 and 8.3 to be learned during their initial education, with Garrhett making the comment that the figures were "a good outcome". The content and structure of the

heuristic (Figure 7.4) was further validated by Brad, who made the comment that the foundational knowledge requisites were, pointing at Figure 7.4, "basically everything that is on this piece of paper".

As a central theme all participants felt that the foundational knowledge requisite commences at the top of Figure 7.4, with the ability to clearly analyse and communicate risk based on threats. Garrhett noted that "every security professional needs to have an understanding of risk". Nick supported this stance explaining that for him risk is the most essential element, stating "I am not talking about a basic level of risk, I am talking about risk where you produce a report based on tangible evidence to tell me what is going on, or what could go wrong, or whatever. Then how we can treat it, to me that is the number one thing I am looking at". The risk view resonated throughout the focus group participants, with Frazer adding (while pointing to Figure 7.4 in the risk discussion) that one of the most essential attributes that is required to be taught is analysis, "it is a core element...you need to teach it early on to people because it applies to all elements, it applies to risk, it applies to identifying what it is that you don't know. If you can't analyse yourself you are not going to actually analyse what information that you need to apply, and that develops the person's attributes in themselves, their confidence etc."

Consistent with Figure 7.4, following the knowledge requisites of risk was the acknowledgement of the necessity for a strong grounding in security theories and principles. These sat within the inference section (Figure 7.4) as planning guides for articulating the security solution, and their co-location and structural placement was supported across the group. Garrhett stated that "they are going to have to know the security concepts and theories like defence in depth, CPTED, as grounding." Again, this view resonated across the group with Brad pointing out that "they lead to core element breakdown in terms of teaching detection etc." Nick concurred with this position, seeing this and the knowledge in this section (inference) as the start of treatment within the risk management framework. According to Nick "treatments are things like your CPTED, situational crime prevention, defence in depth, followed by the physical security elements including security electronics, physical security (barriers), going through all that stuff, it is treatment".

Again reflecting on Figure 7.4 and the knowledge clusters within Figure 8.2, the group saw the requirement for core engineering-focused knowledge underpinning the treatment of security risks for those within the physical security stream. For example, Frazer made the point that it is very important for graduates to have an understanding of the technical side of security treatment. Frazer stated "it's great to do a risk assessment, but unless you understand how the systems work and know the practicalities of them, what the challenges are with them and installing, and how they work to operate, if they don't understand that as well, how can someone say they need to implement that as a mitigation strategy"?

> I would love to see all security consultants have a very good foundation in how the technology actually works. I think it is more important that they have the knowledge of what is possible and what is not, and how to apply it, and they can go to someone else to get the information on how it works. Because a lot of guys that understand the technology in detail can't look at it from the top down, and therefore they don't get the risk that they are trying to mitigate. (Frazer)

Frazer's view triggered agreement across the group with Peter pointing out that "when you talk about the risk treatment, unless you understand what each of these elements (engineering solutions) is in the physical security environment you can't do efficient treatments. Because you don't know whether the treatment is going to be in line with what the threat is, so it has got to balance the threat with what the you would treat it with". Frazer agreed, adding that graduates need to have an understanding of technical variables, locks, access control, CCTV, perimeter detection, their supporting standards and how they tie together.

Brian supported the taxonomy of knowledge, specifically as it relates to security treatments, and stressed that physical security graduates need to understand the goal of individual subsystems, as well as how that subsystem works, how it can be defeated and how quickly this can be achieved. Garrhett concurred and added that graduates also need to know about how subsystems can add value to an organisation and how to impart this information to a client. Garrhett extended this idea using access control as an example "they might be able to say this access control system can actually link into

your human resource management (HR) system, and your building management system so by swiping on here you can turn all your lights on, or by deleting my access rights on this card, or from the HR system then my access is blocked…this card can save you money, time and business process".

Underpinning the engineering requisite knowledge was the requirement for graduates to have a fundamental understanding of the laws of physics and the mathematical principles behind the engineering solution. This point was emphasised by Frazer, Brad and Garrhett. Brad explained that a fundamental understanding of the laws of physics as they apply to light, sound, vibration, movement and inertia was necessary, and related this knowledge to detecting the threat.

Fitting across this knowledge basis was the requisite for sound comprehension of systems theory. Frazer and Peter both strongly emphasised the requirement to teach systems theory as the means for articulating what physical security is about, and how all these individual elements fit together to create a risk mitigation system. Peter stated that "you would have to put systems theory up very high on your criteria".

> Probably one of those foundation units, I think if you taught systems theory like the structure of the degree you come into it and 101 is systems theory. It will help for all these other things (pointing to Figure 7.4) to actually fall into place and be more readily understood by students. (Peter)

Furthermore, the experts also supported the necessity for professional enabling requisites to be clearly articulated in any body of knowledge and taught within a curriculum to ensure students comprehended how broader academic knowledge is used to achieve occupational outcomes. Tied to this supporting knowledge was the engineering design process, or as Garrhett states "the management of the design process". Students need an understanding of the phases that consultants go through to create the end product and also need to understand master planning, concepts, schematic detail design along with how to interact with clients.

Peter noted that this is the same for engineering graduates and that a physical security curriculum should draw from this, "it's the same knowledge, and therefore that

academic knowledge already exists in that (engineering) domain". Frazer also saw the necessity for such knowledge requisites and added other professional practice requisites that were included in Table 7.6 and Figure 7.4. Frazer explained that students needed to learn how to communicate, especially with clients within an engineering function or for general business. He commented about staff who are "fantastic at sitting behind a desk designing the voltage drop between this and this or whatever, but put them in front of a client they are clueless...out of their comfort zone".

There was strong evidence to support the core and supporting knowledge requisites presented in Tables 7.6 and 7.7, along with Figures 7.4 and 8.2 as, according to the experts, all knowledge presented was relevant towards achieving jurisdictional occupational outcomes. The combined phase findings to date highlights a broad and complex body of knowledge for the practice sub-domain of physical security which is characterised by a degree of abstraction in achieving protective security outcomes. However, some knowledge areas already have an extensive body of knowledge and therefore the next consideration is the scope of such knowledge in terms of novice higher education teaching.

9.3.2 Depth and scope of physical security education

The experts all agreed that new graduates were not required to be highly competent professionals and that they should learn the foundations of this broad knowledge base. Given the breadth of learning requisites all agreed that a shallow broad brush approach is the best for educational scope, and consistent with the premises of andragogy (Section 3.7) this needs to be directly focused towards the knowledge necessary to practice. Participants considered that students required grounding in the various subject areas that could be further developed later in professional practice. Peter made the comment that what is needed is a very high level overview, "so somebody can undertake a conversation and contribute to decision making". Brad supported this stance, emphasising the necessity to understand the security theories and principles.

The group strongly believed that the knowledge areas needed goal focus, teaching what students need to practice. For example, sitting within the risk locality within Figure 7.4 was the knowledge category of law. Participants agreed that legal knowledge was a

requisite for physical security professionals, but it needed to be clearly focused. For instance, Garrhett made the comment that it is not necessary to know how the legal system works in fine detail and how to enact a law. What is needed is the ability to interpret legislation or regulations within the security context they are operating within. Nick and Frazer supported this stance, emphasising the requirement to understand legislation, regulations, policies and standards as a legal framework. Garrhett also considered criminology as an area requiring specific scope explaining that he needed to know what his threats are, but not necessarily the criminological basis behind that, such as what motivates them.

> I am not going to be able to influence that they come from a poor family or they have got these other mental problems. I don't need to know any of that. So from my perspective understanding what makes up threat, their motivation and everything else, yes I need to know what makes it up, but I don't need to know the in-depth of what my adversaries are...I don't need to know why people are committing the crime, I don't need to know the root causes, social implications and how we can treat that, I'm not interested in how society can treat that, as a physical security consultant I am not trying to change societies to help them. (Garrhett)

Again Garrhett's views are consistent with the reviewed andragogy literature (Section 3.7) where Knowles (1980, p. 47) work highlighted that for adult education the focus is towards those subjects or topics they see the need to learn, accordant with the knowledge demands of the occupation or profession. An analysis of the group's discussion supports the view that at the undergraduate-novice level, students need the broad fundamental knowledge and how it relates to achieving business objectives securely. As Brad stipulated, "they need a very shallow but broad brush of basically everything that is on this piece of paper" (Figure 7.4).

Nevertheless, Peter did raise the issue of older graduates, explaining that a young graduate is afforded reduced professional expectations than their older counterparts. Peter explained that somebody who already had a working history is expected to operate at a far higher level of professional competence. Peter's views support the embedding of broader professional practice attributes within any undergraduate level program where

school leavers as part of their studies are given their first exposure to professional requirements and how to combine general attributes with core knowledge to operate at a professional level within the paid workforce. According to Peter those students who have already been working in an occupational field would be expected to be demonstrating these attributes in their place of employment, regardless of their graduate status.

9.3.3 Organisation of physical security learning units

The experts were also asked how these knowledge units should be organised. Responses supported a top down approach; Frazer stated "it should be from the top down, first of all you need to understand the risks you are mitigating, and then if you look at it from the other end (lower end) of the spectrum all you are looking at are the laws of physics". Furthermore, Frazer explained that the heavier math or science may be something to deliver later in the course, "in the early stages students should learn the writing side, written communications. Then if somebody needs to pick up their knowledge in math or science you can guide them to do that". Brad added that in the early stages there was the necessity to teach critical and logical reasoning skills as these underpin the scientific process (method)..."if they develop these skills they can teach themselves anything else that is on this paper".

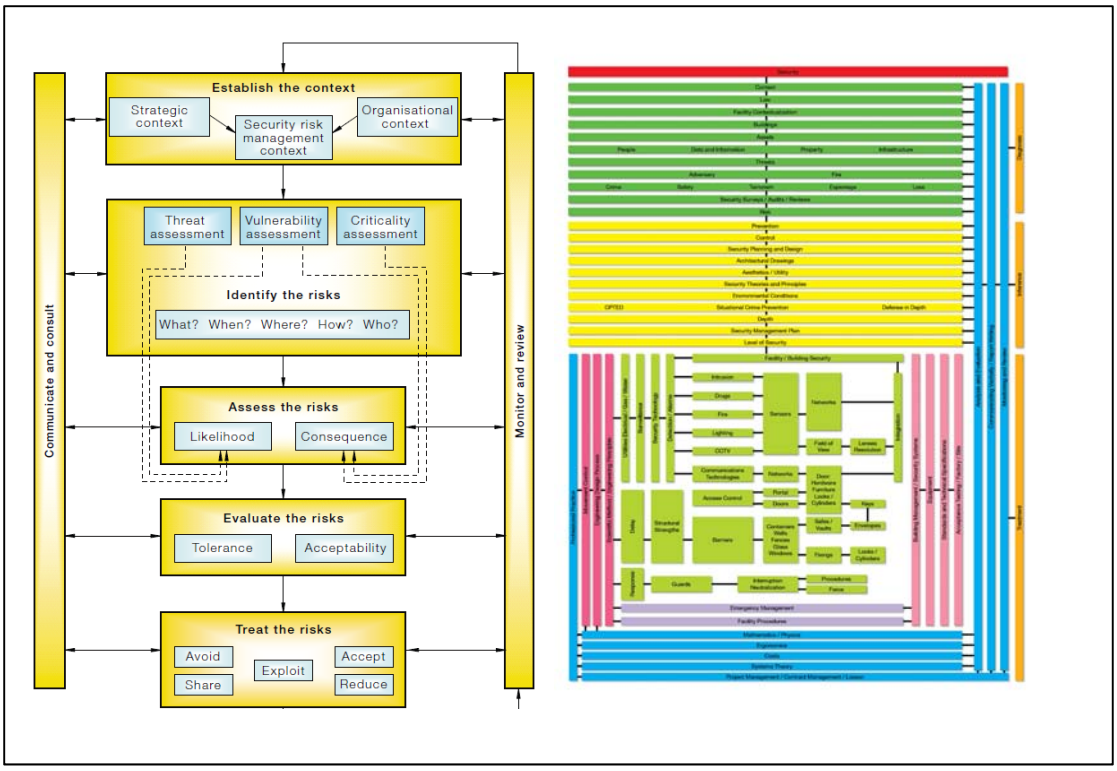
Nick expressed the view that the structure or order of the security course and therefore the learning units should follow the risk management frameworks. So phase one of the course would look at understanding security context, then risk identification and analysis. Treatment would follow including theories and principles including situational crime prevention, CPTED and defence depth, then the treatment elements, detection, delay and response along with project management and other supporting practice knowledge requisites.

Generally there were congruent views that the ordering or course structure of learning units should follow a top down approach accordant with Figure 7.4 and the risk management standards. For example, Figure 9.1 shows the knowledge heuristic sitting side-by-side the risk management framework and process from Standards Australia HB167 Security and Risk Management Handbook. Consistent with Figure 7.4, HB167

presents the diagnoses elements and process within the top section of the framework. Then treatment elements as options are considered at the bottom of the framework. Consensus supported such an approach with focus on the written communications skills early along with mathematics and sciences necessary for understanding the treatment stage of the learning units. Further learning units should be tied to professional practice including project management, contract management and client liaison.

Figure 9.1 Hierarchical ordering for learning units accordant with Figure 7.4 and Standards Australia HB167 Security and Risk Management Handbook process

(See Appendix M)



Consistent with the literature informing the study the experts advocated towards the subject form approach in physical security education. This approach sees knowledge requisites segregated according with their occupational practice of diagnosis, inference or reasoning and treating security problems. Furthermore, more generic concepts and principles combine with core knowledge to form a distinct occupational network of relations. Such findings are consistent with Anderson and Sosniak's (1994) work in terms of sequence and scope of knowledge content. This approach also sits well with

Bloom's work, which according to Anderson and Sosniak (1994, p. 60) expressed that learning should be based on the structure of the domain being learned.

9.3.4 Physical security higher education learning objectives

Further supporting the subject form approach, the consensus across the group was that the learning objectives for physical security should relate to the distinct knowledge areas and how they tie to the overall goal of the sub-domain. Such views support the necessity for an overarching physical security course learning objective, supported by compartmentalised learning objectives across the subjects that make up the body of knowledge. Consistent with the reviewed literature this includes the knowledge of (cognitive), and the ability to apply (behavioural) at a fundamental level, relevant academic knowledge to solve protective security problems.

Furthermore, the learning objectives appeared to follow the top down approach accordant with the organisation of physical security learning units (Section 9.3.3). This approach saw salient learning categories emerge accordant with the work of Abbott and Figure 7.4 (Table 9.3) in terms of the professional practice tasks of diagnosing, inferring about or reasoning, and treating the physical security problem. In addition, a further category emerged that covered knowledge requisites associated with employing academic knowledge to achieve client objectives in a professional setting, this category was labelled professional practice. Accordingly, Table 9.3 presents the relationship between the professional's occupational task, its underpinning physical security knowledge content areas and their associated learning objectives as indicated by the experts.

Table 9.3 Relationship between the professional tasks, knowledge areas and associated learning objectives

Professional Practice Task	**Knowledge Requisites**	**Objectives**
Diagnosing	Concept of security	Understand what is denoted by the word security
	Law	Interpret legislation (Acts & regulations)
	Security Risk Management Security assessments: Surveys/audits/reviews	Identify, analyse and evaluate security risks Communicate risk
Inference	Role and objectives of physical security	Macro system objectives: Understand how to reduce opportunity, increase difficulty and neutralize threat
	Prevention approaches : Security theories: defence in depth, CPTED, situational crime prevention, zoning, protection in depth/layers; detect/delay/respond, systems theory	Understand how protection can be achieved Comprehend physical security theories and principles
	Human factors in security	Understand how people interact and influence security
	Physical security planning and design	Understand how to develop and present a security management plan and concept design
Treatment	Sub-system technical knowledge	Goals of sub-system components
	Electronic security sub-systems: Detection, access control, surveillance	Understand how they: Operate (math & physics, electrical theory), how they are defeated and how long/difficult, what this means for planning and design, when to use what and why, and how to apply technical standards to sub-system components
	Physical sub-systems: Delay/difficulty	Understand how they: Operate (math & physics), how they are defeated and how long/difficult, what this means for planning and design, when to use what and why, and how to apply technical standards to sub-system components
	Response: Procedural sub-system	Understand how system components integrate through procedures and practices to achieve objectives
Professional Practice	Information analysis	Be able to critically analyse information
	Business communication skills	Be able to produce written reports Be able to present information verbally
	Design management Project management Contract management	Understand how to plan, organize, monitor and communicate to achieve deliverables
	Research skills	To know when to seek , and how to find further information

Table 9.3 highlights that physical security's learning objectives relate to the knowledge requisites to contextualise and diagnose the security risk problem, the theories, practices and principles used to plan for managing the threats that pose a risk and the engineering knowledge requisites to design, implement and commission a protection system. Table 9.3 also highlights that professional practice knowledge is required for graduates to understand how functional outcomes are achieved in the professional setting.

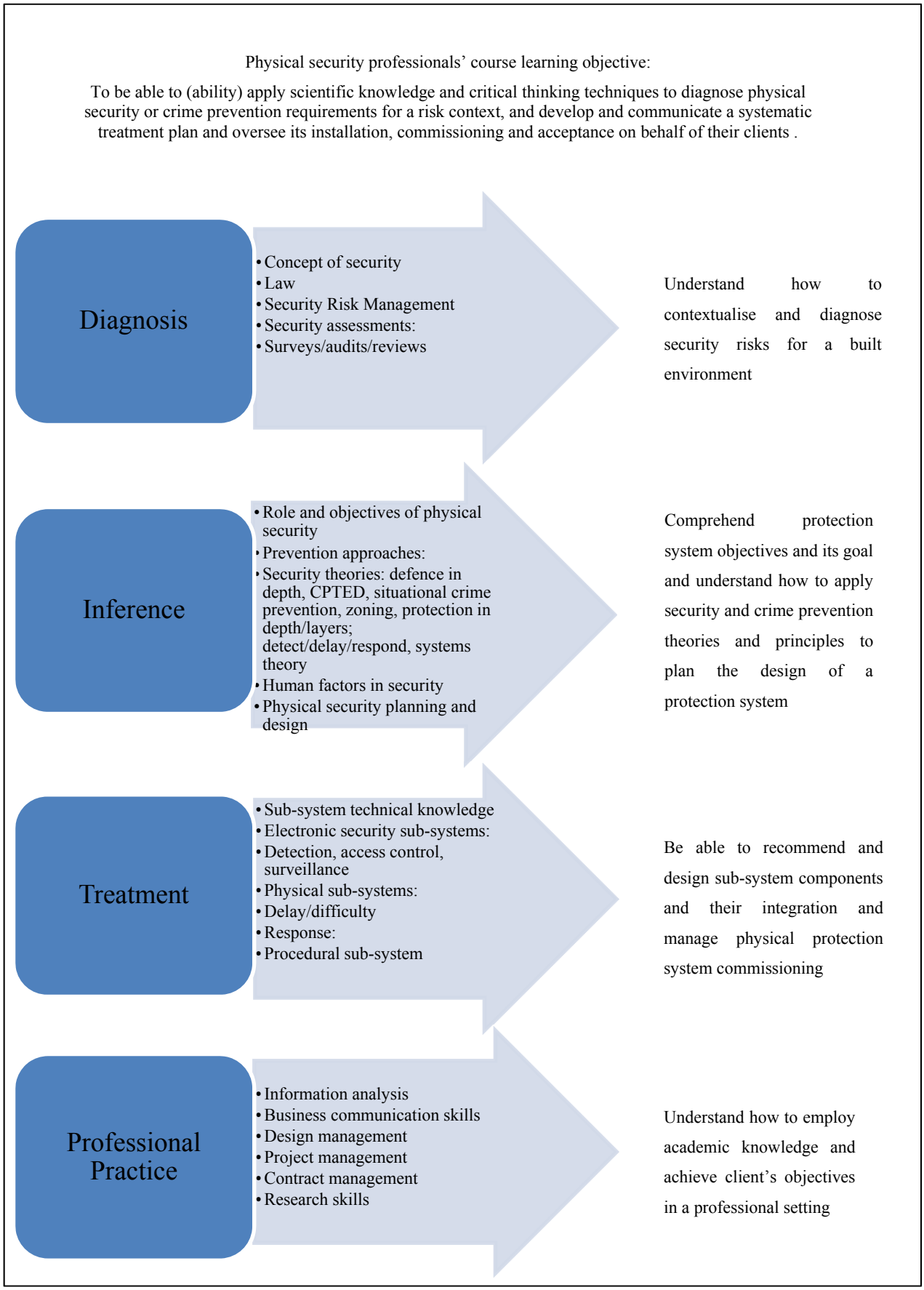
9.4 Phase Four: Interpretation

Phase Four sought to test a number of key assertions developed from the pilot study and respond to the question: *What are the knowledge requisites and supporting learning objectives for physical security professionals*?

Assertion 1 of the pilot study proposed that heuristics representing the propositional knowledge and distinct networks of relations amongst the various theories, concepts, principles and practice components or elements for physical security professionals can be developed for enhancing reception learning. In principle, Assertion 1 was supported; however, the experts highlighted some limitations with the current knowledge heuristic (Figure 7.4), commenting that while they find it very useful, novices would have trouble interpreting what it actually means for physical security education. Peter explained that students would benefit from a flow chart that actually breaks the hierarchical system down (Figure 9.2). Garrhett supported this approach highlighting that in the engineering firms, as part of their graduate programs, they have flow charts that show how the program ties together and that the intentions of this study would benefit from such an approach.

Therefore, the group recommended the development of a simpler flow chart that clearly communicated the professional knowledge task roles, their knowledge content and supporting learning objectives. Such views and an analysis of the focus group discourse led to the development of Figure 9.2 a physical security body of knowledge flow chart. This chart indicates how the occupational task roles and their underpinning educational knowledge category requisites relate to compartmentalised learning objectives, how they are segregated, what they encompass and how they serve the achievement of the broader professional outcomes post-graduation for novice learners when considered against a holistic course learning objective.

Figure 9.2 Physical security knowledge system flow chart



Assertion 2 of the pilot study proposed that a desirable knowledge system for physical security professionals relates to core foundational physical security and crime prevention knowledge along with general academic knowledge that underpins professional work. Accordingly, the focus group questionnaire asked participants a distinct question relating to the make-up of the qualitative heuristic (Figure 7.4) and MDS map (Figure 8.2). Findings from Phase Four support Assertion 2 and as an iteration found that Tables 7.6 and 7.7 along with Figures 7.4 and 8.2 represent such a knowledge system. The experts agreed that Figures 7.4 and 8.2 iteratively present compelling foundational knowledge structures. As Brad stated earlier, "the knowledge and skills requisites are a very shallow but a broad brush of basically everything that is on this piece of paper" (Figure 7.4).

Assertion 3 of the pilot study proposed that the course learning objective and therefore educational goal for a physical security professional can be phrased as "an ability to apply scientific knowledge and critical thinking techniques to diagnose physical security or crime prevention requirements for a risk context, and develop a systematic treatment plan and communicate their evaluation to clients". However, based on the expert's views, assertion 1 was only partially supported as the experts in Phases Two and Four of the study highlighted the requirement for professionals to be able to project manage the installation, commissioning and acceptance testing of the system on behalf of their clients. This led to the deductive development of a broader course learning objective:

To be able to (ability) apply scientific knowledge and critical thinking techniques to diagnose physical security or crime prevention requirements for a risk context, and develop and communicate a systematic treatment plan and oversee its installation, commissioning and acceptance on behalf of their clients.

In addition, the experts indicated that physical security's knowledge basis should be supported through subject specific knowledge requisites relating to professional practice roles and sub-system goals. Drawing on the works of Abbott, participants' responses to the order and structure of the knowledge system and the analysis techniques of Spradley, this thematically related to diagnosis, inference, treatment and professional practice requisite knowledge. Such a structured learning curriculum is indicated in

Table 9.3, which highlights how the sub-domain's knowledge structure is compartmentalised according to these thematic occupational roles matching with the subject form approach.

Assertion 4 of the pilot study proposed that physical security education needs to include both a science and arts approach to include the physical and social sciences that underpin the higher strata tasks of the professional domain. This assertion was supported by the experts in Phase Four. For instance, Garrhett made the comment that he has observed two different types of personality in security consulting, those who prefer technology and those who prefer report writing.

> You've got people who just like technology and come from a technical side and you've got people who prefer report writing and writing frameworks and management procedures and it is not just in security. It is almost like a different personality or trait of the individual and trying to merge them together into one person, it is very difficult to find someone to hire who has both those skills in their personality who is willing to do that. In our team we will basically hire technical people and we'll hire report writers and put them into the same team because they need to bounce off each other's skills. (Garrhett)

Frazer supported this view explaining that report writing should be developed early on in the course, then as the students' progress, introduce them to the more technical mathematics and physics focused subjects. This emphases the importance of communication in the physical security domain. Such a position is congruent with the organisational of physical security learning units (Section 9.3.3) discussion emphasising a top-down approach. There was strong support from the experts that physical security's curriculum should be a combined arts and science approach where the arts approach is emphasised initially, throughout the teaching of risk and security theories and principles. This would include critical thinking skills, analysis techniques and written and verbal communication skills. Then as the course moves into the treatment focused learning units students should be exposed to the science and math underpinning treatment variables.

9.5 Phase Four: Reliability and trustworthiness

The focus group discussion was recorded and transcribed as per the writing of Schensul, LeCompte, Nastasi and Borgatti (1999), enabling close and repeated analysis of the data for interpretation. In addition, participants were asked to write down their own learning objectives on note pads, which were later scanned in (Appendix I) for further analysis, providing a chain of research evidence. Furthermore, an independent note taker was also included in this phase, whose notes (Appendix J) were used for cross referencing key themes emerging from this phase of the study. Combined these approaches established trustworthiness and validity in Phase Four's outcomes.

Reliability of Phase Four also embedded Maxwell's (1992, p. 283) work, where descriptive and interpretative validity combined provided confidence in the focus group analysis. For qualitative research Maxwell (1992, p. 284) explained that validity is not a sole product of any methodology, rather it pertains to the data accounts, or conclusions reached. Descriptive validity was achieved again using a narrative account of what participants said, supported by the typed transcripts to instill trustworthiness. Then, interpretative validity was again achieved through the use of participant's own language, relying as much as possible on participant's own words and concepts (Maxwell, 1992, p. 289).

Furthermore, reliability and validity were broadly embedded into the mixed-methods design as it applied methodological triangulation using different methods and/or types of data to study the same research question. In this approach the strength of one method offset potential weakness within others (Fraenkel, Wallen & Hyun, 2012, p. 559) where data was continually taken back to the experts for validity of interpretation. For instance, experts' opinions explaining the structural map of physical security's body of knowledge was drawn on to explain and validate the structural representations towards articulating a shared, desirable body of knowledge within the participant sample.

9.6 Conclusion

This chapter presented Phase Four of the study, explaining what the knowledge concept categories and their cultural structure (mean for the future of physical security education. Section 9.2 introduced Phase Four's participants, highlighting the depth of physical security knowledge each member of the focus group brought to the study. Then

Section 9.3 presented an analysis of the focus group's discussion. This section highlighted what the experts believed the desirable curriculum attributes were for future physical security professionals based on the individual phase findings. Section 9.4 then presented an interpretation of Phase Four's findings, responding to Phase Four's research question through a series of assertions brought forward from the pilot study. The interpretation of Phase Four was supported by a discussion of phase reliability and trustworthiness in Section 9.5, and the chapter concluded in Section 9.6.

Phase Four highlighted that physical security has a complex, yet abstractly structured system of knowledge. This system is made up of discrete knowledge concept categories and supporting professional level skills which combine with other knowledge requisites to produce the sub-domain of physical security's work. Each core knowledge category has its own body of knowledge, underpinned by a structured model of learning or scientific basis which must be learned by novices as it provides the academic basis for the sub-domain's knowledge system. Such knowledge is organised accordant with professional role tasks including diagnosing, reasoning about or inferring, and treating society's protective security problems and is supported by discrete learning objectives which are tied to a broader sub-domain learning objective. Such learning objectives represent what is desirable for graduates to know prior to graduating and recognise that deeper learning occurs during professional development post-graduation.

Chapter 10: Study interpretation, limitations and recommendations

10.1 Introduction

The study sought to conceptualise the knowledge requisites and their cultural structure for the emerging profession of physical security. Such concept reduction was achieved through a series of iterations embedded into distinct research phases. This chapter presents an interpretation of the study (Section 10.2), presenting a response to the study's overarching research question, supported by individual phase outcomes Section 10.3 then links the study's finding to its research objectives set in Chapter 1 (Section 1.6). This section is supported in Section 10.4 through a discussion of the study's findings and explaining their significance for security professionalism. The chapter also presents, in Section 10.5, a number of research limitations that may have had an impact on the findings across the various phases.

The chapter also discusses reliability and validity (Section 10.6) across the study, presenting measures embedded into each phase to increase the value and generalizability of findings. Section 10.7 then presents future research recommendations including the need for research into a consensual language base for security and also the need for further body of knowledge research to provide cross cultural replication for the study's findings. Also discussed is the necessity for a comparative analysis of physical security course curriculum and this study's findings to overcome inconsistencies to produce a more mature knowledge system. Outcomes of this study suggest that the recognition of physical security as a specific jurisdictional occupational category for security professionals should be supported. The chapter and study then concludes with Section 10.8.

10.2 Interpretation of the study

The study was developed to overcome the dearth of knowledge pertaining to physical security as a sub-domain practice area or cultural paradigm within the professional sector of security's occupational stratum. Through a review of pertinent literature physical security as a distinct sub-domain was acknowledged as a jurisdictional practice area within the broader security domain (Section 3.3). Yet little research has been undertaken to highlight the knowledge requisites, how they should be communicated structurally and their supporting learning objectives to produce a group of persons in

command of a dependable body of knowledge to solve society's protective security problems.

10.2.1 Overarching research question and study outcomes

The study's design and methodology, through a series of phase research questions, sought to respond to the question: *What is a desirable knowledge system (body of knowledge) for physical security professionals as conveyed through the published literature and accessible professionals?*

In response to the study's research question findings support that a desirable knowledge system for physical security professionals relates to core foundational physical security and crime prevention knowledge (as listed in Tables 7.6 & 7.7 and Figures 7.4 and 8.2) braced by general academic attributes that underpin professional work. Congruent with Abbott's (1988) work, these tables and figures present a complex, abstract, yet systemised body of knowledge. This body of knowledge comprises individual categories of knowledge which are interdependent yet interrelated with all other categories related to the cover term security. Each category has its own distinct body of literature that when combined facilitates the physical security sub-domain's work.

The study's overarching research question sought to develop a shared paradigm for the cultural domain of physical security. The study found that a physical security professional's body of knowledge is made up of categories of knowledge associated with diagnosing the security or crime problem, core security theories and principles to plan and design a protection strategy (inference). It also includes engineering or more technically focused knowledge to design a treatment system, including product selection along with other professional knowledge to undertake the project through to completion. Such professional knowledge includes professional liaison and project management requisites. This combined knowledge system enables physical security professionals to liaise and coordinate with other professionals and specialists to achieve the security outcome. Consistent with Figure 10.1 this includes liaising with architects, planners and engineers, along with occupational security providers (See Table 1.2) to achieve their work goals (Figure 10.1). As Abbott (1988, p. 8) asserted, for professionals the techniques themselves may be delegated to other workers, and it is this

delegation which, accordant with Abbott's (1988, p. 9) views, makes the physical security professional a professional.

Figure 10.1 Physical security professional's liaison and coordinating roles with other professionals and specialists to achieve security outcomes

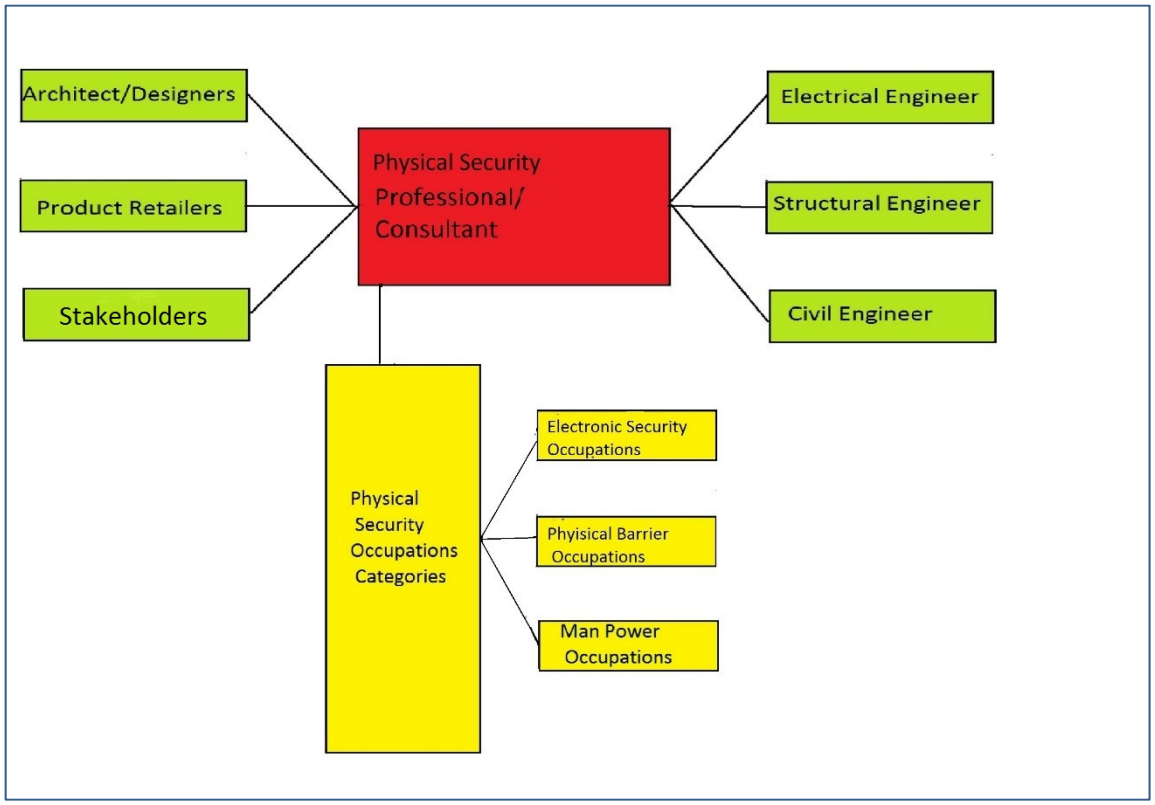


Figure 10.1 indicates that the body of knowledge for a physical security professional is that which facilitates the achievement of the treatment system including the linking together of various stakeholders to achieve the security solution, but not its ongoing operational management. The operational management would be considered the role of security management (See Chapter 3). This interpretation of physical security's knowledge system is congruent with the reviewed literature informing the study (Chapters 2 & 3) and specifically Abbott's (1988) work which stated that "only a knowledge system governed by abstraction can redefine its problems and tasks, defend them from interlopers, and seize new problems…Abstraction enables survival in the competitive system of professionals (p. 9).

10.2.2 Individual study phase research questions

By means of a constructivist design, the combined research phase sub-questions and their supporting objectives sought to sequentially build knowledge to facilitate a response the study's overarching research question.

10.2.2.1 Phase One: Knowledge category exploration

Phase One of the study was the initial exploratory phase and extracted the salient knowledge concept categories from physical security and non-traditional (general) security's printed domain to respond to the question: *What are the explicit knowledge concept categories for physical security represented as repeated themes printed in security texts and their structure?*

A response to this question saw the development of Table 6.18 presenting Phase One's salient knowledge concept categories. This included both core physical security and some supporting professional enabling knowledge categories.

This phase also sought to develop an initial ethnographic structural table representing a folk taxonomy as a form of spatial knowledge indicating cultural structure to be used for the development of a knowledge domain heuristic. This aspect of the study drew on the work of Spradley (1979), incorporating his ethnographic analysis technique which displays the relationships among all concept categories in a domain, illuminating subsets and the way these subsets are related to the domain as a whole. For this study such analysis revealed internal, local structure that is often tacitly below the surface within a culture.

Therefore, a response to Phase One's research question also saw the development of Table 6.19 and Figure 6.2 presenting a first iteration systematic knowledge structure for the sub-domain of physical security organised based on a single semantic relationship with the cover term security.

Phase One highlighted that physical security, and security more generally, does have a broad albeit dispersed, knowledge corpus and cultural structure. However, this knowledge base lacks both unanimity and does not link to clear educational outcomes with only one reviewed text - Security science: The theory and practice of security

(Smith & Brooks, 2013) - having clear chapter outcomes that could be considered educational objectives. This text presented a clear intent, "to help facilitate regularity and internal consistency within the knowledge domain of security science by bringing theories and principles from other disciplines into the security domain's knowledge corpus". However, while each chapter in the book clearly outlines an objective or set of objectives for security professionals or students, these objectives relate only to that topic included within that chapter. There is no single overarching set of educational objectives for the entire text. Consequently, Phase One presented the first step in this research endeavour to link physical security knowledge, its structure and supporting learning objectives to an overarching learning goal or objective as a system within a clear jurisdictional context.

10.2.2.2 Phase Two: Knowledge category expert enrichment

Phase Two of the study was an additional exploratory phase aimed to enhance the knowledge category corpus (Table 6.18) and further develop the folk taxonomy and (Table 6.19) shared knowledge heuristic (Figure 6.2). Through semi-structured interviews, this phase drew on security experts as constructors of knowledge (Section 4.3), to respond to the question: *What are the implicit knowledge categories, and instinctive structure by security experts in achieving physical security risk mitigation not extracted from the literature?*

The methodology and procedure for this phase stemmed from the work of Cohen, Manion and Morrison (2000, p. 267) who emphasised that knowledge is often generated between people through conversation and Spradley (1979, pp. 138-142) who advocated the use of structural questions to elicit the relationship among parts of a culture and their relationship with the whole.

Phase Two saw the experts identify an additional 43 knowledge concept categories, to produce Table 7.5, covering knowledge that graduates would benefit from an understanding of prior to commencing their professional apprenticeships. A response to Phase two's research question resulted in the expert's additional knowledge categories being combined with Phase One's findings. This analysis produced Phase Two's

enhanced knowledge concept category taxonomy (Table 7.6), resulting in 98 desired knowledge areas for graduate physical security professionals to be abreast of.

The experts also provided opinion on the structure of the knowledge base, guiding the placement of more ambiguous categories within the folk taxonomy and its supporting heuristic and embedding a confidence level towards Phase One's outcomes.

A response to Phase Two's research question saw the re-development of the folk taxonomy reflecting the expert's opinions, which, through the analytical procedures of Spradley (1979), led to the development of Table 7.7 a hierarchical folk taxonomy. This then led to the development of Figure 7.4, Phase Two's physical security knowledge heuristic. An analysis of Figure 7.4 highlights that from a qualitative standpoint physical security's professional knowledge requisites range from the diagnosis of security concerns (diagnosis), through to planning and designing security solutions (inference), through to the commissioning of these physical security solutions (treatment). This core knowledge is braced by professional enabling knowledge such as communication. As the experts noted, and is highlighted in Figure 7.4, there is a clear need for physical security professionals to understand the entire physical security process.

Phase Two of the study also saw the experts highlight that the division of labour diagram (Figure 1.1) for physical security professionals must represent the parallel professional engagement required to achieve large security projects where physical security professionals must sit alongside other professionals, including architects and engineers and so on to fulfil the client's requirements. According to the experts, a body of knowledge for a physical security professional must include a holistic knowledge basis that embraces a combined arts and sciences approach as the professional must understand the science which underpins the engineering solution as well as the social sciences illume the problem.

10.2.2.3 Phase Three: MDS knowledge description

Phase Three sought to overcome some of the limitations in Phase Two's qualitative analysis by representing prominent concept categories in n-dimensional space. A limitation identified in Phase Two was the subjectivity and difficulty in locating

spatially some concept categories in relation to other categories. As John stated in his interview, “not all relations between concepts will be linear”. This phase of the study uncovered the psychometric structure of physical security’s knowledge base in response to the question: *What is physical security’s knowledge content structure as measured by multidimensional scaling?*

To respond to Phase Three’s research question significant concept reduction was required as it was acknowledged that all 98 knowledge concept categories couldn’t be subjected to an MDS analysis. Accordingly, drawing on the folk taxonomy as a guide (Table 7.7) core and some subordinate concept categories were extracted to produce Table 8.5, registering 24 salient physical security knowledge categories to be subjected to MDS analysis.

In response to Phase Three’s research question Figures 8.2 (MDS clusters) and 8.3 (MDS dimensional orderings) were developed. Figure 8.2 highlighted that the knowledge basis for physical security is organised based on similarity grouping of requisite knowledge for producing the profession’s work. For instance, Cluster One (Figure 8.2) related to knowledge used to diagnose and reason about (inference) the security problem. Cluster Two co-located knowledge associated with the physical retardation of an adversary’s progression, to delay their attack’s headway for a period of time. Then Figure 8.3 indicated some congruence with dimensional analysis, locating those knowledge categories associated with treatment high on the treatment scale. However, this was not as clear for diagnosis, with those knowledge categories clustered in the centre. Nonetheless, Figure 8.2 provided a degree of validation for Figure 7.4, showing similar clusters of knowledge in n-dimensional space as those co-located in Figure 7.4. The similarity between the two Figures indicates congruent validity for the different phase outcomes.

A comparative analysis of Figure 7.4 and 8.2 suggests that physical security’s knowledge structure relates to clusters of similar or highly related categories of knowledge associated with diagnosis the security problem, reasoning or inferring about it about it to produce a conceptual plan to treat the problem, and engineering or technical knowledge required to achieve a functional solution on behalf of the client.

This core knowledge is braced by more general professional practice knowledge used to produce the profession's work.

10.2.2.4 Phase Four: Physical security's knowledge evaluation

Phase Four of the study sought to understand this uncovered knowledge for physical security from an educational perspective, and sought to respond to the question: *What are the knowledge requisites and supporting learning objectives for physical security professionals?*

A response to Phase Four's research question supported a subject form approach for physical security education, tied to an overarching learning objective (Figure 9.2) as a systemised educational program. Phase Four indicated that physical security education should relate to the distinct knowledge areas that combine to achieve the profession's work and how they tie together. The experts expressed that a curriculum for physical security should be organized and taught in subject form as a combined arts and sciences underpinning, from a top down approach. Such organisation in subject form should include the knowledge required to diagnose the security problem, covering subjects including the concept of security, the law as it relates to pursuing security and security risk management. Such subjects should be supported by learning objectives that emphasize an understanding or ability to undertake diagnosis of the problem and communicate their diagnosis to their client.

The experts also articulated that following risk, professional inference knowledge should be taught which relates to core security and security planning theories and principles that facilitate a conceptual solution to the security problem. Supporting this knowledge were key learning objectives relating to the macro-system objectives (treatment), understanding how people interact with security and how to develop and present a security management plan. The group emphasised that hierarchically this knowledge would predominately follow an arts approach. Then, once students have the foundational knowledge they should be presented with the more technical engineering knowledge that teaches them how to produce the treatment system. This knowledge would include the mathematics and physics underpinning the engineering tools, devices and systems used to achieve a functional state of security. The experts conveyed that

this part of the curriculum would follow a sciences approach and supported by clear learning objectives which demonstrate academic understanding of the subject matter.

The group also highlighted the necessity of introducing at later stages students to the foundational knowledge required for professional practice such as project management. They also recognised that some academic knowledge skill sets should be embedded into all categories of requisite knowledge teachings. These included general academic attributes such as critical analysis skills along with communications skills both written and verbal. Phase Four supported both the knowledge requisites as those communicated through Figures 7.3 and 8.2 of the study, and that the teaching of subjects should follow a systemised structure from diagnosis to treatment along with professional practice to form a curriculum template for higher education in the area of physical security.

10.2.2.5 Phase Four: Test of pilot study assertions

Phase Four highlighted how knowledge was built on the basis of previous knowledge across the distinct phases within the study. Phase Four also provided the ability to test a number of key assertions developed from the pilot study.

Assertion One, that heuristics (Figures 7.4, 8.2 and 8.3) representing the propositional knowledge and distinct networks of relations amongst the various theories, concepts, principles and practice components or elements for physical security professionals can be developed for enhancing reception learning, was supported by the focus group experts. A number of experts did, however, express the desire for a simpler flow chart connecting the professional task roles, knowledge requisites and supporting learning objectives. This request consequently led to the development of Figure 9.2 a flow chart of physical security's knowledge system. Nonetheless, all focus group participants supported the ability and suitability of the knowledge heuristic to display the knowledge requisites and its internal structure for the domain of physical security.

Assertion Two considered that a desirable knowledge system for physical security professionals relates to core foundational physical security and crime prevention knowledge (as listed in Tables 7.6 & 7.7 and Figures 7.4 and 8.2) braced by general academic attributes that underpin professional work. Assertion Two was supported by the focus groups participants.

Assertion Three expressed that the course learning objective and therefore educational goal for a physical security professional can be represented as: “an ability to apply scientific knowledge and critical thinking techniques to diagnose physical security or crime prevention requirements for a risk context, and develop a systematic treatment plan and communicate their evaluation to clients”. The principles within this assertion were supported; however, minor changes were required to reflect the views of the experts throughout the study. Findings support that a more holistic learning objective would include that professionals need the ability to oversee, or project manage, the achievement of the treatment system. Consequently, the course learning objective was changed to reflect this view:

To be able to (ability) apply scientific knowledge and critical thinking techniques to diagnose physical security or crime prevention requirements for a risk context, and develop and communicate a systematic treatment plan and oversee its installation, commissioning and acceptance on behalf of their clients.

Assertion Four expressed the view that physical security education needs to include both a science- and arts-based approach to include the physical and social sciences that underpin the higher strata tasks of the professional domain. Assertion Four was well supported across the group, with all experts emphasising such a required approach for higher education.

10.3 Study objectives

The study met a number of research objectives (Section 1.6). Firstly, through a constructive process it developed a first iteration consensual knowledge map (Figure 7.4) presenting the organisational structure of the physical security domain’s broad knowledge concepts. This map can act as a domain heuristic for articulating the occupational role concept knowledge areas and their supporting knowledge basis within physical security’s body of knowledge. In addition, through Figures 7.4 and 8.2 the study provides visual clarity for security practitioners and professionals to understand where their individual expertise fits into the physical security domain within a holistic systems approach. It also provides the means of explicitly presenting the hierarchical knowledge areas and their subordinate concepts of physical security to tertiary students towards enhancing their efficiency of learning (reception learning).

For educators the findings of Phase Four also highlight desirable learning objectives for future physical security professionals, showing a direct link between that to be learned and its fit with professional practice. The study highlights a broader desired learning objective as a first iteration, supported by subject specific professional competencies for physical security educators in institutions of higher learning to draw on in their curriculum planning. As Kevin stated in the pilot study, "there must be a direct link between the knowledge requisites, the curriculum and the intended work".

10.4 The significance of codified knowledge for security professionalisation

Many new professions are emerging across contemporary society, but their emergence and eventual social designation as professional occupational groups is both a challenging and extensive undertaking. Emerging professional domains must convincingly uncover their knowledge base to persuade the public and legal arenas of its complexity and necessity to be a product of higher education along with the requisite for it to be recognised in the group phenomenon as a profession.

Social recognition of a profession is tied to many sociological facets, including the degree of consensus or sharing of beliefs pertaining to theory, methodology, techniques and problems as these elements represent the very essence of any established professional paradigm or cultural domain (Lodahl & Gordon, 1972). As Zipser (1991, p. 1) points out, professional work is judged according to the standards of a reasonably competent qualified person holding that skill. Accordingly, for professionalisation, a key element in any paradigm's maturity is the degree of consensus in its application of theory, methodology and techniques underpinned by its content and structure (Lodahl & Gordon, 1972, p. 66). Consequently, the work of Lodahl and Gordon (1972, p. 66) highlighted that more developed paradigms have more structure and thus more predictability than fields with less developed paradigms, with structural maturity related to their professional maturity. Physical security as a cultural paradigm is relatively unevolved when compared to more traditional academic fields such as physics. The indication to date suggests that security and more specifically physical security is therefore a long way from becoming formally recognized as a profession.

From a structural standpoint much of the security domain within the law and order paradigm (non-traditional) resides at the operational end of security's occupational

stratum (Figures 1.1 & 10.1), with diminutive recognition for the professional category membership or understanding of occupational role. Central to security's emergence and acceptance by both the public and legal arenas for the higher end of the occupational stratum as a profession is its evidence of a valid body of abstract knowledge that requires formal education through institutions of higher learning. As Axt (2002, p. 142) notes, it is not those within the security industry to decide if security is a profession, but the beneficiaries and consumers (public). To achieve such recognition evidence must support that as with other professional occupations, security requires the employment of a dedicated body of structured knowledge underpinned by core academic skills requisite of the higher educational system.

Griffiths, Brooks and Corkill (2011, p. 2) expressed that for professional security knowledge to be useful it must be clear in terms of its practices. ASIS divides the non-traditional security domain within the law and order paradigm into four distinct disciplines: physical security, information security, personnel security and information security (Horrocks, 2001, p. 218). However, Talbot and Jakeman (2009, p. 55) consider security management as an additional, yet distinct overlapping discipline area, and refer to these as practice areas. Physical security is recognised by many authors (Section 3.1) and experts (Chapter 6) as a clear, distinct jurisdictional knowledge area. However, reasonable questions remain, is physical security a distinct sub-domain requiring its own knowledge base? Can those focusing in this jurisdictional area be considered professionals? Johnston and Warner (2014) allude to the view that it isn't, but has the potential to be.

Based on the literature informing the study (Chapters 2 & 3), for physical security to be a profession there must be a clear academic base (Horrocks, 2001), one of a complex, abstract nature (Abbott, 1988); that is built on a transmittable body of knowledge (Horrocks, 2001, p. 220) representing content and structure. According to Horrocks (2001, p. 224) this provides the mechanisms by which the body of knowledge is reviewed, refined and developed. The Hallcrest report on private security and police in America acknowledged that security constitutes a specialised area of knowledge, but this knowledge base is unclear and requires substantial research. If we accept that, consistent with the reviewed literature, physical security is an area of specialized practice, then it must have a codified knowledge base that can be generalised and

transmitted. The Australian Interim Security Professional's Task Force (2008) states that those considered to be security professionals are required to take responsibility for security projects in the far-reaching sense. However, there is a lack of understanding in terms of knowledge and competencies required for such persons (p. 4).

Sennewald (2013, p. 7) stated that "in the security consulting sphere security professionals engage in a process, a problem solving process, in which the consultant must first identify the problem(s), gather available data pertaining to the problem(s), analyse that data, and then offer advice in the form of recommendations that will solve, cure or otherwise minimize the problem(s)". These views highlight that if physical security is to be recognised in the group phenomenon as a clear jurisdictional sub-domain, then it must be supported by an academic basis and associated competencies that directly align to the group's work, that are transmitted to novices through the higher educational fraternity. Higher education bears the primary responsibility for the development of human resources in all fields, and accordingly, security is no exception (Rogers, Palmgren, Giever & Garcia, 2007, p. 1).

The knowledge based view underpinning professionalism resonates within the literature of professionalism (Section 2.3). Accordingly, focused security knowledge can be developed from security concepts (Smith, 2002). A way of exploring this knowledge base is to understand the knowledge concepts through the detection of repeated themes within the sub-domain and broader domain, categorising it based on similarity and contrast and organising it hierarchically (Section 1.8) to produce a structure. Formal structure provides the means for understanding knowledge requisites in relation to work goals, the ordering of knowledge in education for building understanding and reinforcement, and competencies to take into professional apprenticeships post-graduation from institutions of higher learning.

Prior to the findings of this study, physical security could be located optimistically in its pre-paradigmatic stage at best, lacking explicit consensus in its jurisdictional distinction of roles, its articulation of theory, methodology and underpinning knowledge basis. Consequently this study sought to overcome the lack of evidence in the literature regarding physical security knowledge and structure required to be taught by institutions of higher learning and mastered by professionals.

The investigation was undertaken through a cultural domain analysis. This investigated the content and structure of the physical security sub-domain that sat subordinate to the cover term security. This was necessary for security to move along the professionalisation path within the jurisdictional area of physical security. Informed by a significant breadth and depth of literature the study did not seek a perfect solution, to the question to the study's overarching research question. Instead it sought a first iteration desirable body of knowledge for future security professionals.

The study developed a folk taxonomic table (Table 7.7) representing the cultural domain of physical security, which led to the development of Figure 7.4, representing content along with its local relations as a knowledge heuristic. Such taxonomies are not static, they are dynamic and with further focused research they will change, but as Cliff said (Chapter 5), "you have to start somewhere". The study therefore produced a first iteration knowledge corpus (Table 7.6) and heuristic structure (Figure 7.4). This hierarchical structure was supported by psychometric maps (Figures 8.2 & 8.3) which help communicate what makes up the complex abstract knowledge base for physical security. The ethnographic table (Table 7.7) and heuristic tool (Figure 7.4) along with psychometric maps (Figures 8.2 & 8.3) provide an initial body of knowledge indicating the content and structure for the physical security sub-domain.

The study's outcomes exemplified a medical model for understanding physical security knowledge content and structure. The adoption of a medical model for understanding security's body of knowledge is not a unique approach when considering security within the non-traditional-crime prevention paradigm. For instance, Lab (2014, p. 28) described crime prevention in terms of a public health model where prevention strategies are classified as primary, secondary or tertiary. Lab notes that crime science fits well within the public health prevention model, and therefore the use of a health model of professional practice for understanding physical security's knowledge structure is logical.

Such an outcome has important significance for physical security professionalism and education. Firstly, professions require a high degree of standardized educational criteria, as students require the requisite knowledge to practice upon graduation, and this requires uniform educational standards. Furthermore, this must include a broad working

knowledge of the entire spectrum of professional practice (Fox, 1994, p. 203). Wilensky's (1964, p. 138) influential work emphasised this point, explaining that the success or claim for professional standing is greatest where the society evidences strong wide spread consensus regarding the knowledge or doctrine to be applied.

Professional knowledge standardization involves the substance, or more formally, the stored information, which is the body of accepted knowledge in a field, with the objective to cover all of the profession's important content (Lodahl & Gordon, 1972, pp. 61-62). In addition, enhanced learning occurs through understanding the structure of knowledge within the context of the professional field (Finley, Nam & Oughton, 2011). From an educational standpoint All, Huycke and Fisher (2003) explained that the ability to put information together in meaningful ways improves both retention and understanding. For retention purposes the storage of information in a manner which facilitates meaning, and therefore practice, is a cognitive process. Remembrance is enhanced by encoding information from short term memory into long term memory. Such encoding is reinforced by cognitively constructing concepts, propositions, schema and visual images, promoting meaningful learning. Accordingly, Tables 7.6, 7.7 along with Figures 7.4 and 8.2 present an initial body of knowledge for the physical security sub-domain representing knowledge requisites and epistemological structure that can be standardised and taught across a diverse range of institutions of higher learning, with teaching organised based on their structural principles consistent with Figure 9.2.

Figure 9.2 provides clear direction for understanding how knowledge requisites and their structure directly relate to the jurisdictional work of this emerging profession. This provides clarity for both students to understand how knowledge requisites relate to their future employment and helps educators plan course materials, learning sequences and competency assessments. According to All, Huycke and Fisher (2003, p. 312) when methods of meaningful learning are used, students and teachers report increased ability to retain knowledge over time and find ways to connect new information with more general previously learned materials. Key factors associated with meaningful learning includes: 1) assimilation of new concepts and propositions into existing cognitive structures, 2) knowledge organised hierarchically in cognitive structures, and 3) subsumption of concepts and propositions into existing hierarchies. Meaningful learning

occurs when the learner begins to understand the similarities and differences (dissimilarities) in concepts and ideas.

The background significance of the study (Section 1.6) highlighted that evidence based research will play an important role in the professionalisation of security. This discourse articulated that professionals must have the requisite knowledge learned through training in the arts or science, or both, and supported by clear learning objectives commensurate with their area of foci to produce higher strata work. The study produced codified representations of cultural knowledge which include the salient important content for the sub-domain of physical security (Table 7.6), along with both local connections (Figure 7.4) and macro structure (Figure 8.2) as tools for understanding knowledge concept categories and their relations with other categories, separated based on similarity and differences.

The development and use of structural tools for enhancing learning in an academic domain are supported in the work of Gonzalvo, Canas and Bajo (1994, p. 601), who highlighted that research supports the differences between expert's and novice's representations of knowledge. However, as novice learners study a discipline their knowledge of structural arrangements becomes more consistent with the experts (Gonzalvo, Canas and Bajo (1994). Therefore presenting the knowledge structure (presented learning) rather than requiring students to discover it over time is a more efficient means of knowledge transfer (Ausubel, Novak & Hanesian, 1978, p. 26). The outcomes of the study therefore significantly contribute to the professionalisation of security education. The study's outcomes offer the means to build consensus and ultimately standardise security curriculum, and enhanced instructional means, resulting in stronger confidence in graduate's abilities to undertake their professional roles in a competent and professional manner.

Furthermore, in developing standardised education such structures can be used as planning maps to reveal curriculum, course and lesson planning and provide in depth study guides for learners (All, Huycke and Fisher, 2003, p. 313). Adult learners have the potential to be self-directed, therefore an important teaching task is to develop connections between the abstract world of concepts with the real world of experience to facilitate such learning (Gitterman, 2004, p. 96). The study findings therefore enhance

the security domain's ability to communicate to society the depth and complexity of physical security's knowledge base, as well as develop structural representations of this knowledge to enhance reception learning for novices and provide planning tools for security educators.

There is a vast body of literature supporting the requirement for emerging professions to provide such a detailed description of their knowledge base. Such a body of knowledge must cover the important subject matter of the domain. This may be in taxonomic structure or some other form that enables understanding of the areas of knowledge, tied to its jurisdictional work. Security if it is going to emerge as a recognised profession must embrace this literature and pursue its knowledge base through targeted research. As only once the higher end of the security stratum can demonstrate through research and practice the necessity of a formal knowledge system, what this includes (content) and associated competency assurances can a case be made for regulation of the industry to exclude those who do not possess evidence of such learning. Such a body of knowledge as uncovered in this study must be that which can be standardized and accepted across pertinent institutions of higher learning. Only then can security progress through the professionalisation process and eventually emerge as an accepted profession. Therefore the findings of this study significantly contribute to physical security's professional journey, although they must be accepted cognisant of various research limitations.

10.5 Limitations of the study

It is important to note the methodological limitations of this research. These include the lack of clear definitions of security terminology, a limited understanding of what constitutes a security professional, small sample sizes in terms of research participants and reviewed texts and the use of deductive analysis by the researcher. Despite this, measures and considerations were taken to ensure the reliability and validity of research results.

10.5.1 The modern day physical security professional

There is limited understanding of the modern day physical security professional. As the literature informing the study (Section 2.2) highlighted, the very concept of security

lacks agreed definition and this lack of clarity permeates through the occupational stratum of security. Manunta (1999) pointed out this is due to the concept of security meaning different things to different people. Therefore, the study focused on what is denoted by the word security to understand its cover term and professional context instead of providing a singular agreed definition to guide the research outcomes. An analysis of this literature led to the premise that security denotes protection from adverse effects of threat, where functionally it is the pursuit of such protection.

The study then contextualised this understanding to the practice area of physical security, articulated as activities directed towards the diagnosis, inference and treatment system of security or loss coupled risk concerns manifested through unlawful access or crime enablers, or both. Physical security aims to implement control measures in a delineated environment to mitigate risk associated with an expressed threat (Section 3.3). Combined the expression of what is denoted by the word security and the designation of physical security as a distinct practice area guided the selection of experts. In the absence of clear articulation of what constitutes a physical security professional the inductive and deductive analysis underpinning such phraseology and the selection of experts based on such articulations may have negatively impacted the findings of the study with regards to responder bias, and this must be acknowledged as a potential limitation within the study.

10.5.2 Language

The use of language within the study, specifically the use of security terms, has a degree of subjectivity and must therefore be acknowledged as a limitation within the study. Security lacks precise language (Manunta, 1999) and as such clear definitions of extracted terms limit the findings of the study. Nevertheless, it must be acknowledged that in the early days of research we need to know first what it is we seek to define. Brooks (2008, p. 154) acknowledged this issue also in his study of the knowledge domain of security risk management. Brooks made the point that his study did not attempt to provide precise concept definition thus allowing the experts to define their own understanding through relationship of concepts or knowledge structure. Accordingly, the findings of the study present knowledge concept categories and areas

suitable for further research including clear operational definitions congruent with the context of the security domain.

10.5.3 Data corpus

The data corpus for Phase One of the study was limited to 15 published security texts. It must be acknowledged that this is a small printed sample and did not include journal published papers. However, arguably 15 texts do represent a sound sample for the detection of repeated themes when considered from the annotated bibliographic intent of these texts. As intended by the methodology, this provided an initial data corpus for cuing experts' stored implicit knowledge towards identifying additional knowledge concept categories and supporting content which they believe, on the basis of their experience, are important knowledge requisites for security graduates when commencing their professional apprenticeships. While the data corpus was small, it was focused and captured salient themes that were supported by the experts.

10.5.4 Expert sample

Experts were drawn on to provide both raw data and also verify the findings or interpretations (member checking) at various stages in the study. However, the sample size for each phase could have been larger to improve the findings and the ability to generalise these findings. Each sample group within the study introduced a potential bias and degree of error into the study's findings. This was of note in Phase Three of the study (MDS analysis) where sample limitations meant only 29 complete surveys were analysed due to incomplete questionnaires and poor participation. However, Phase Three provided a confidence analysis between the qualitative concept map (heuristic) (Figure 7.4) and MDS clusters (Figure 8.2) where this analysis supported the structures found in Phase Two and Three with a high degree of similarity in graphical outcomes. Nonetheless, findings must be considered in relation to the relatively small participant sample sizes within the study's phases.

10.5.5 Deductive analysis

The ethnographic approach required a degree of deductive analysis without the aid of mathematical relations. Such analysis is not without its biases and errors. A comparative

analysis between the deductive analysis structure (Figure 7.4) and MDS analysis (Figure 8.2) indicated a degree of concordance, with similar concepts clustered together across both graphical representations. However, there was still a degree of subjectivity within the ethnographic analysis which must be acknowledged.

10.6 Reliability and validity

Reliability and validity of the bibliographic extraction stemmed from the use of published in-print text books as the data corpus which according to Silverman (2002, p. 229) are, in principle, reliable sources for analysis (Silverman, 2002, p. 229). In addition, the software program NVIVO9 was used to enhance the validity of the count analysis, producing an objective calculation of word occurrences and providing objective knowledge concept categories external from the researcher (Liamputtong & Ezzy, 2006, p. 274). In addition, this data extraction and knowledge structure was tested through expert interviews providing an additional degree of validation (Appendix D).

Reliability and validity associated with qualitative data derived from interviews and focus groups was achieved through both descriptive and interpretative validity techniques embedded into the interview analysis process, an approach which stemmed from Maxwell's (1992, p. 283) work. Descriptive validity was established through the use of a narrative approach which included using participant's responses (Appendix K) to interview questions as quotes in text. This also led to interpretative validity as conclusions drawn relied as much as possible, on participant's own words and concepts (Maxwell, 1992, p. 289). In addition, where possible outcomes were taken to other participants within the study providing a degree of verification through member checking (Creswell & Miller, 2000).

Further, all interviews and focus group discussions were transcribed verbatim and included in the study's appendices for reference (Appendix K, L), thus providing trustworthiness and validity. The transcription of all interviews and focus groups enabled close and repeated analysis of the data (Schensul, LeCompte, Nastasi & Borgatti, 1999).

The focus group validity in the principle was also enhanced through the use of an independent note taker, who recorded salient points for later analysis (Appendix F). In

addition, participants were asked to write down their learning objectives on note pads provided which were later scanned in (Appendix I) for further analysis, forming a chain of research evidence. Combined this approach established trustworthiness and validity for the focus groups outcomes.

Validity of the MDS analysis included an assessment of the covariance between extracted concepts from the concept reduction process (Table 8.5) and the underlying construct of Physical security, providing a validity assessment of the MDS source data. For the principal study Cronbach's Alpha produced a high ($\alpha = .913$) value, indicating sound reliability and validity for Phase Three survey questionnaire knowledge concept categories. This was slightly lower than the pilot study measure ($\alpha = .945$), perhaps due to a larger number of concepts analyzed in the pilot study. Reliability was demonstrated through the goodness-of-fit. This was evaluated according to Kruskal's Stress formula 1 and the Squared Correlations. The data presented a Stress score of 0.24399 and an RSQ of .70566 (Squared correlations in distances), which according to the MDS Stress measure, not all concepts were in their ideal spatial locality. Nevertheless, a stress score of 0.24399 is well within the 0.54 stress score tolerances of Rakshit and Ananthasuresh (2008, pp. 293-294).

Reliability and validity across the study were embedded into the mixed-methods design as it applied methodological triangulation (triangulation) using different methods and/or types of data to study the same research question. In this approach the strength of one method offset potential weakness within others (Fraenkel, Wallen & Hyun, 2012, p. 559). This included the use of data extraction from texts, expert enrichment supported by a qualitative ethnographic technique and MDS analysis. Both the ethnographic technique and MDS analysis produced similar results. In addition, during the study data was continually taken back to the experts for validity of interpretation. For instance, experts' opinions explaining the structural map of physical security's body of knowledge was drawn on to explain and validate the structural representation towards articulating a shared, desirable body of knowledge within the participant sample during Phase Four of the study.

10.7 Future research

The literature review highlighted that not all occupational roles will be acknowledged as professions. Professions are a social designation, with formal recognition tied to a sufficiently complex, abstract body of knowledge. This body of knowledge is underpinned by academic materials drawn from science or some constructed model of social organisation. This knowledge must have a degree of mystique for the lay person, yet crucial for society to function well, and organised based on jurisdictional cultural boundary. In considering this body of literature and the findings from the study there are a number of research recommendations towards enhancing security's journey through the professionalisation process, to emerge as a recognised profession underpinned by robust research and education.

10.7.1 Security language research

Security has been acknowledged as a distinct, although diverse field of study (Brooks, 2007), which, as with other professional fields, draws knowledge from many different academic domains. However many of these fields have sought to list and define their concepts or terms within the context of their domain's work to enhance professional application of their body of knowledge. Security has not achieved a reliable level of concept definition as found in the more mature professions. This lack of clarity impedes robust research and ultimately professional consistency in how the domain applies its work. Jaques (1989, p. 7) work expressively stressed the necessity for common language in order to undertake robust research within academic domains. Security would benefit from an in-depth study reviewing and defining security terms that can be published as a single source reference text. Such research would significantly progress security along the professionalisation path.

10.7.2 Cross cultural replication

The study drew on a research sample of experts who practice as physical security consultants (professionals) in Australia, but also provide advice for international projects. Nevertheless, it must be acknowledged that the sample may have embedded an Australian centric cultural bias when highlighting the knowledge requisites, structural properties of the knowledge system and bracing learning objectives. This usage may

have manifested in the cultural nuances in thought processes underpinning how the knowledge is used. For instance, Figure 8.6 presents the similarities between Figure 7.4 and Figure 8.2. However, in Figure 8.2 barriers sits numerically higher than delay based on summated ratings of dissimilarity in the MDs analysis; whereas in Figure 7.4 delay appears before barriers along the physical variables arm of the treatment strategies.

Nevertheless, the MDS analysis was based on an international sample of participant's summated ratings of perceived dissimilarity and may therefore better represent the thought processes in how the knowledge is used to solve security problems. However, the security domain would significantly benefit from cross further cultural refinement of Figure 7.4, and the testing of all 98 concept categories using MDS. It would also benefit from further testing of Assertion Three with a larger, pancultural research sample. This would provide another iteration of the knowledge base and add a higher degree of generalisability to the knowledge structure.

10.7.3 Physical security course validity

The study produced what can be considered as a desirable body of knowledge as represented in Figures 7.4 and 8.2 for the sub-domain of physical security. Nevertheless, security educators would benefit from a comparative analysis of these figures with institutions of higher learning physical security curriculum. This would analyse the topics and structure representing the curriculum underpinning their courses across the physical security sub-domain and compare these to the findings of this study. Such an analysis would highlight any discrepancies between the findings of this study and what is being taught towards facilitating a common knowledge base for educators and graduates moving into this sub-domain stream. The importance of this should not be overlooked. As Edmondson's (1995) work found, for developing curricula for interdisciplinary domains where content from several disciplines must be integrated, concept maps are an effective tool.

From an educational standpoint, concept maps provide the means for mapping the content in such a way to facilitate consensus on how to design interdisciplinary courses and promote more meaningful learning. According to Edmondson (1995, p. 779) the extent to which educators identify specific content to be learned is an important element

in the development and implementation of a curriculum as is the extent to which the content can be organised. Edmondson expressed that for medical education the concept map approach to curriculum development provided an effective conceptual framework and theoretical basis for implementing an innovative approach to education (p. 781), stating "concept mapping facilitates theory-driven curriculum development that is grounded in learning theory and proven in practice" (p. 792). A vast body of literature supports the argument that physical security education and the professionalisation process for security would benefit from the adoption of such an approach to curriculum development, supported by consensual learning objectives. Therefore an in-depth comparative study is essential for physical security educational requirements to be standardised and accepted across different institutions of higher learning.

10.7.4 The recognition of physical security as a jurisdictional category

The notion of the security professional is being pressed by the security industry. However in the Australian context this group of individuals is not formally recognised in Australia according to Australian Bureau of Statistics (ANS) data, ABS labour force data and licensing industry categories (Table 1.2) (Prenzler, Earle & Sarre, 2009, p. 3) (Section 1.3). This is in contrast with the Australian Security Professionals Interim Task Force's designation of this group as those persons working at the higher strata of the operational sector and in the strategic sector of the security industry (2009). The only category of persons fitting with the notion of the security professional is the Security Consultant (Table 1.2).

However, an Independent Commission Against Corruption (ICAC) report in NSW (2013) noted, the role of the security consultant in achieving security project outcomes is poorly defined, and potentially leads to corrupt practices. It is therefore recommended that the security professional be formally recognised in the Australian Bureau of Statistics (ANS) data, ABS labour force data and licensing industry categories; where inclusion is based on a relevant tertiary qualifications and experience that meets the criteria as set by the Australian Security professionals Registry. In addition, Table 1.2 does not acknowledge physical security barrier providers as an occupational category. Yet many in the work force are employed to install physical barriers for security

purposes. As such, it is recommended that this group of people are also recognised as security occupational persons.

10.7.5 The development of a crime prevention jurisdictional category for security professionals.

The study highlighted that physical security is a sub-domain requiring specialised knowledge, with much of it stemming from the engineering domain. However, the reviewed literature and interviewed experts acknowledged there are personnel within the professional strata stream of the security domain who engage with clients to solve crime problems, yet do not apply such engineering knowledge per se. Accordant with the work of Clarke (1992, p. 5) (Section 1.4.1) such persons would diagnose the crime problem using a problem centred approach, then identify and test possible solutions.

Lab (2014, p. 32) (Section 3.7) introduced the notion of such professionals and referred to an emerging domain of crime science as their knowledge basis. Lab's work explained the emerging domain of crime science as a discipline that focuses on attacking crime in society utilizing a broad range of disciplines, employing an extensive array of tools to control, influence or manipulate the social and physical environment in the fight against crime. This introduces another potential sub-domain stream or practice area within the security domain. Such a domain appears to encompass a diverse knowledge focus rather than more specialised engineering knowledge to solve crime problems in the protection of assets. Therefore it is recommended that further research is undertaken to explore the potential for this practice area to emerge within the professional strata of the non-traditional security domain.

10. 8 Study conclusion

The literature suggests that for an occupation to be defined as a profession there are a number of criteria that need to be met. Alongside social recognition, having a distinct body of knowledge and being included as a discipline in the higher education domain are part of the requirements of profession recognition. These requirements have not yet been met for the sub-domain area of physical security. However, all professions including the prestigious ones of medicine and law were practiced for centuries before they became codified and formally regulated, set apart from other occupations due to

their need for specialised knowledge (Criscuoli, 1988, p. 99). As Criscuoli points out, security, as with other occupations, is not just a matter of intuition or common sense, it involves a complex body of knowledge, analytical ability, along with the ability to prescribe appropriate security measures for individually specific circumstances (1988, p. 99). The study therefore undertook a cultural domain analysis of the physical security domain to map out the knowledge requisites and its structure, and to determine what should be included in a higher education course on physical security and accordingly has important implications for physical security education and professionalism.

The study used a mixed method approach, drawing on qualitative and quantitative research techniques in a constructivist paradigm to determine the existence of a body of knowledge for physical security. Such a body of knowledge was found to be represented through Figures 7.4, 8.2, and 9.2. For physical security, the study has a number of implications. The study found that as premised in the reviewed literature, there subtly exists a branch of learning relating to the diagnosis of, and reasoning about society's protective security and crime prevention problems. This learning also includes the application of validated techniques underpinned by scientific knowledge to treat these concerns. Individuals schooled in this jurisdictional branch of knowledge go by various names, including among others, security consultants or advisors (Section 1.4) and their learning is often enhanced through occupational apprenticeships. The study demonstrated their knowledge can be formally codified and therefore consistently taught, which as a system of knowledge would include a combined arts (social sciences) and sciences approach. Such codification would impart the ability to critically analyse available data to diagnose and reason about the methodology drawing on social science frameworks and techniques, along with the requisite engineering knowledge required to recommend and implement treatment systems, underpinned by mathematics and science as a department of learning. Such learning also requires highly developed graduate attributes such as communication skills to facilitate professional work.

Such a model of learning fits with the security science definition offered by Smith and Brooks (2013, p. 21), articulated as "a discipline that brings together broader discipline concepts into a structured body of knowledge, integrating them into a single domain boundary". However, while this literature alludes to a discipline structured according to a single domain boundary, the findings of this study conclude that security science

represents a broader domain discipline label, where sitting subordinate to this label are various specialised knowledge areas of jurisdictional boundary. One such boundary area is the practice domain of physical security, which as Johnston and Warner (2014, p. 13) note, is an area in and of itself that can be studied in a rigorous and scholarly manner. This study's findings support this view and found that both the ethnographic qualitative technique and MDS concept mapping were valid tools for developing and representing physical security's body of knowledge.

Johnston and Warner (2014, p. 13) asked "where are the (university) degrees in physical security"? The lack of degrees within the knowledge domain of physical security is not surprising given the lack of understanding pertaining to the knowledge requisites, its structure and supported learning objectives. In the significance of this study it was argued that the concept of the security professional will be better understood through research driven domain exploration that presents validated higher education curriculum and associated competency measures. As an outcome this was premised to increase the broader public's understanding and confidence in physical security professional's knowledge and services and gain such trust towards recognition as professionals. The study found through Figure 7.4, Figure 8.2 and Figure 9.2 that a clear jurisdictional knowledge corpus exists that can be codified and linked to educational objectives to develop such degree courses. Such a course would represent an opportunity to gain greater professional recognition for physical security professionals.

The substantiation of physical security as a jurisdictional sub-domain or cultural paradigm within the professional sector of security's occupational stratum with a distinct body of knowledge and learning basis represents the first step towards consistency in practice within the security domain. Security is emerging as a new profession, and physical security as a new sub-domain, and this study represents a significant step forward in this professionalisation journey, helping establish in the group phenomenon the physical security professional within the broader group of security professionals.

References

Abbott. (1988). *The system of professions: An essay on the division of expert labor*. Chicago: The University of Chicago Press.

All, A. C., Huycke, L. I., & Fisher, M. J. (2003). Instructional tools for nursing education: Concept maps. *Nursing Education Perspectives, 24*(6), 311.

Allan, J. (1996). Learning outcomes in higher education. *Studies in Higher Education, 21*(1), 93-108. doi: 10.1080/03075079612331381487

Allen, P., & Bennett, K. (2012). *SPSS statistics: A practical guide version 20*. South Melbourne, Vic.: Cengage Learning Australia.

American Institute of Architects. (2001). *Building security through design*. Washington, DC: American Institute of Architects.

American Institute of Architects. (2004). *Security planning and design: A guide for architects and building design professionals*. Hoboken, NJ: John Wiley and Sons.

Anderson, L. W., & Sosniak, L. A. (1994). *Bloom's Taxonomy: A forty-year retrospective*. Chicago: National Society for the Study of Education.

Anderson, P. (2007). *Education in security*. Sydney: Macquarie University.

ASIS International. (2009). *Facilities physical security measures guideline*. Alexandria, VA: ASIS International.

Atlas, R. (2013). *21st Century security and crime prevention: Designing for critical infrastructure protection and crime prevention* (2nd ed.). Boca Raton, FL: Taylor & Francis.

Atlas, R. I. (2008). *21st century security and CPTED*. Boca Raton: Auerbach

Australian Interim Security Professionals Task Force. (2008). *Advancing security professionals: A discussion paper to identify the key actions required to advance security professionals and their contribution to Australia*. Canberra: Author.

Ausubel, D. P. (1968). *Educational psychology: A cognitive view*. New York: Holt, Rinehart and Winston.

Ausubel, D. P., Novak, J. D., & Hanesian, H. (1978). *Educational psychology: A cognitive view* (2nd ed.). New York: Holt, Rinehart, and Winston.

Axt, D. A. (2002). Is private security a profession? *Security Management, 46*(8), 142.

Baker, P. R., & Benny, D. J. (2013). *The complete guide to physical security*. Boca Raton: CRC Press.

Baldwin, D. A. (1997). The concept of security. *Review of International Studies, 23*(1), 5-26. doi: 10.1017/s0260210597000053

Balnaves, M., & Caputi, P. (2001). *Introduction to quantitative research methods: An investigative approach*. London: Sage.

Barnett, R. (1994). *The limits of competence : Knowledge, higher education, and society*. Buckingham: Open University Press.

Beccaria, C. (1775). *An essay on crimes and punishments* (2nd ed.). Brookline Village, MA: International Pocket Library.

Bédard, J., & Chi, M. T. H. (1992). Expertise. *Current Directions in Psychological Science, 1*(4), 135-139.

Bernard, H. R., & Ryan, G. W. (2010). *Analyzing qualitative data: Systematic approaches*. Thousand Oaks, CA: Sage.

Bertalanffy, L. V. (1968). *General system theory: Foundations, development, applications.* New York: G. Braziller

Boreham, P., Pemberton, A., & Wilson, P. (Eds.). (1976). *The professions in Australia: A critical appraisal*. St. Lucia: University of Queensland Press.

Borg, I., & Groenen, P. J. F. (2005). *Modern multidimensional scaling: Theory and applications*. New York: Springer.

Borodzicz, E. P., & Gibson, S. D. (2006). Corporate security education towards meeting the challenge. *Security Journal, 19*(3), 180-195. doi: 10.1057/palgrave.sj.8350016

Bowen, H. R. (1955). Business management: A profession? *The Annals of the American Academy of Political and Social Science, 297*(1), 112-117. doi: 10.1177/000271625529700115

Breakwell, G. M., Hammond, S., & Fife-Schaw, C. (2000). *Research methods in psychology*. London: Sage Publications.

Broder, J. F., & Tucker., E. (2012). *Risk analysis and the security survey* (4th ed.). Waltham, MA: Butterworth-Heinemann.

Brooks, D. (2008). *The development and presentation of psychometric concept maps within the knowledge domain of security risk management*. Doctor of Philosophy, Curtin University of Technology, Perth, WA.

Brooks, D., & Corkill, J. (2012). The many languages of CCTV. *Australian Security Magazine*, February/March, 57-59.

Brooks, D. J. (2007). *Defining security through the presentation of security knowledge categories*. Paper presented at the 7th Australian Security Research Symposium, Perth.

Brooks, D. J. (2010). What is security: Definition through knowledge categorization. *Security Journal, 23*(3), 225-239.

Brooks, D. J. (2011). Security risk management: A psychometric map of expert knowledge structure. *Risk Management, 13*(1/2), 17-41.

Brooks, D. J. (2012). A psychometric technique to develop consensual concept maps to aid science education. *International Journal of Modern Education Forum, 1*(1).

Brooks, D. J. (2013). Corporate security: Using knowledge construction to define a practising body of knowledge. *Asian Criminology(8)*, 89-101. doi: 10.1007/s11471-012-9135-1

Bruner, J. S. (1977). *The process of education*. London: Harvard University Press.

Burstein, H. (1996). *Security: A management perspective*. Englewood Cliffs: Prentice-Hall.

Caballero-Anthony, M. (2008). Non-traditional security and infectious diseases in ASEAN: Going beyond the rhetoric of securitization to deeper institutionalization. *The Pacific Review, 21*(4), 507-525. doi: 10.1080/09512740802294523

Carter, R. (1985). A taxonomy of objectives for professional education. *Studies in Higher Education, 10*(2), 135-149. doi: 10.1080/03075078512331378559

Chi, M. T. H., Farr, M. J., & Glaser, R. (1988). *The nature of expertise.* Hillsdale, NJ: Lawrence Erlbaum Associates.

Clarke, R. V. (1992). *Situational crime prevention: Successful case studies*. New York: Harrow and Heston

Clements, K. (1990). *Toward a sociology of security*. Boulder: University of Colorado.

Cogan, M. L. (1955). The problem of defining a profession. *Annals of the American Academy of Political and Social Science, 297*(1), 105-111. doi: 10.1177/000271625529700114

Cohen, L., Manion, L., & Morrison, K. (2000). *Research methods in education* (5th ed.). London: Routledge.

Colak, A. A., & Pearce, J. (2009). 'Security from below' in contexts of chronic violence. *IDS Bulletin, 40*(2), 11-19. doi: 10.1111/j.1759-5436.2009.00017.x

Contos, B. T., Crowell, W. P., DeRodeff, C., Dunkel, D., Cole, E., & McKenna, R. (2007). *Physical and logical security convergence: Powered by enterprise security management*. Burlington, MA: Syngress

Coole, M., & Brooks, D. J. (2009). *Security Decay: An entropic approach to definition and understanding*. Paper presented at the 2nd Australian Security and Intelligence Conference

Coole, M., & Brooks, D. J. (2011). *Mapping the organizational relations within physical security's body of knowledge: A management heuristic of sound theory and best practice.* Paper presented at the 4th Australian Security and Intelligence Conference, Citigate Hotel, Perth, Western Australia.

Coole, M., Corkill, J., & Woodward, A. (2012). *Defence in depth, protection in depth and security in depth: A comparative analysis towards a common usage language.* Paper presented at the Australian Security and Intelligence Conference, Perth, WA.

Coole, M. P. (2010). *Theory of entropic security decay: The gradual degradation in effectiveness of commissioned security systems*. Masters of Science, Edith Cowan University.

Corkill, J., & Coole, M. P. (2013). *Security, control and deviance: Mapping the security domain and why it matters*. Paper presented at the 6th Annual Australian and New Zealand Critical Criminology Conference, Hobart.

Cotterell, L. E. (1984). *Performance* (2nd ed.). East Sussex: John Offord.

Cotterrell, R. (1984). *The sociology of law: An introduction*. London Butterworths.

Craighead, G. (2003). *High-rise security and fire life safety* (2nd ed.). Woburn, MA: Butterworth-Heinemann.

Creswell, J. W., & Miller, D. L. (2000). Determining validity in qualitative inquiry. *Theory into Practice, 39*(3), 124-130. doi: 10.1207/s15430421tip3903_2

Criscuoli, E. J. (1988). The time has come to acknowledge security as a profession. *Annals of the American Academy of Political and Social Science, 498*(1), 98-107.

Cunningham, W. C., & Taylor, T. H. (1985). *The Hallcrest report : Private security and police in America*. Portland, Or.

Daley, B. J., & Torre, D. M. (2010). Concept maps in medical education: An analytical literature review. *Medical Education, 44*(5), 440-448. doi: 10.1111/j.1365-2923.2010.03628.x

Davies, P. M., & Coxon., A. P. M. (1982). *Key texts in multidimensional scaling*. London: Heinemann Educational.

Day, J. M. (1994). *Plato's Meno in focus*. London: Routledge.

DeGroot, A. D. (1966). Perception and memory versus thought. In B. Kleinmuntz (Ed.), *Problem solving: Research, method and theory*. New York: Wiley.

Dhami, M. K., & Harries, C. (2009). Information search in heuristic decision making. *Applied Cognitive Psychology, 24*(4), 571-n/a. doi: 10.1002/acp.1575

Donald, A. S. (1983). *The reflective practitioner: How professionals think in action*. New York: 1983.

Eburn, M. (2005). *Emergency law : Rights, liabilities and duties of emergency workers and volunteers* (2nd ed.). Leichhardt, NSW: Federation Press.

Eden, C. (1988). Cognitive mapping. *European Journal of Operational Research, 36*, 1-13.

Edgar, A. D., & Ifantis, K. (2007). What kind of security? *Internation Journal, 62*(3), 450-456.

Edmondson, K. M. (1995). Concept mapping for the development of medical curricula. *Journal of Research in Science Teaching, 32*(7), 777-793.

Eisner, E. W. (1979). *The educational imagination: On the design and evaluation of school programs.* New York: Macmillan

Epstein, R. M., & Hundert, E. M. (2002). Defining and assessing professional competence. *JAMA: The Journal of the American Medical Association, 287*(2), 226-235.

Eraut, M. R. (1994). *Developing professional knowledge and competence*. London: Falmer Press.

Ericsson, K. A., & Charness, N. (1994). Expert performance: Its structure and acquisition. *American Psychologist, 49*(8), 725-747.

Ericsson, K. A., & Charness, N. (1997). Cognitive and developmental factors in expert performance. In R. R. Hoffman, K. M. Ford & P. J. Feltovich (Eds.), *Expertise in context : Human and machine* (pp. 3-39). Menlo Park: AAAI Press.

Ericsson, K. A., & Chase, W. G. (1982). Exceptional memory. *American Scientist, 70*(6), 607-615.

Ericsson, K. A., & Kintsch, W. (1995). Long-term working memory. *Psychological Review, 102*(2), 211-245.

Fayol, H. (1984). *General and industrial management*. London: Pitman.

Fennelly, L. J. (2003). *Effective physical security* (3rd ed.). Burlington: Elsevier.

Fennelly, L. J. (2012). *Handbook of loss prevention and crime prevention* (5th ed.). Waltham, MA: Butterworth-Heinemann.

Fennelly, L. J. (2013). *Effective physical security* (4th ed.). Waltham, MA: Butterworth-Heinemann.

Finley, F. N., Nam, Y., & Oughton, J. (2011). Earth systems science: An analytic framework. *Science Education, 95*(6), 1066-1085. doi: 10.1002/sce.20445

Fischer, R. J., & Green, G. (2004). *Introduction to security* (7th ed.). Boston: Butterworth Heinemann.

Fischer, R. J., Halibozek, E., & Green, G. (2008). *Introduction to security* (8th ed.). Burlington, MA: Elsevier.

Fischer, R. J., Halibozek, E., & Walters, D. (2013). *Introduction to security* (9th ed.). New York: Elsevier.

Flexner, A. (1915). *Is social work a profession?* Paper presented at the National Conference of Charities and Corrections, Baltimore, Maryland.

Fosnot, C. T. (1996). *Constructivism: Theory, perspectives, and practice.* New York: Teachers College Press.

Fosnot, C. T. (2005). *Constructivism: Theory, perspectives, and practice* (2nd ed.). New York: Teachers College Press.

Fox, R. E. (1994). Training professional psychologists for the twenty-first century. *American Psychologist, 49*(3), 200-206.

Fraenkel, J. R., Wallen, N. E., & Hyun, H. H. (2012). *How to design and evaluate research in education*. New York: McGraw-Hill.

Fraser, K. M. (1993). *Theory based use of concept mapping in organization development: Creating shared understanding as a basis for the cooperative design of work changes and changes in working relationships*. Ann Arbor: UMI.

Freidson, E. (1970). *Profession of medicine: A study of the sociology of applied knowledge*. New York: Harper & Row.

Freidson, E. (1973). *The professions and their prospects*. Beverly Hills, CA: Sage Publications.

Freidson, E. (1988). *Profession of medicine: A study of the sociology of applied knowledge*. Chicago: University of Chicago Press.

Garcia, M. L. (2000). Personal opinion: raising the bar for security professionals. *Security Journal, 13*, 79–81.

Garcia, M. L. (2001). *The design and evaluation of physical protection systems*. Burlington, MA: Butterworth-Heinemann.

Garcia, M. L. (2006). *Vulnerability assessment of physical protection systems*. Burlingham, MA: Elsevier.

Garcia, M. L. (2008). *The design and evaluation of physical protection systems* (2nd ed.). Burlington, MA: Butterworth-Heinemann.

Gigerenzer, G., & Gaissmaier, W. (2011). Heuristic decision making. Annual Review of Psychology, 62(1), 451-482. doi: 10.1146/annurev-psych-120709-145346

Giguère, G. (2006). Collecting and analyzing data in multidimensional scaling experiments: A guide for psychologists using SPSS. *Tutorials in Quantitative Methods for Psychology, 2*(1), 27-38.

Gill, M., & Howell, C. (2012). *The security sector in perspective: A security research initiative report*. Leicester Perpetuity Research & Consultancy International.

Gillespie, B. J. (1981). Professionalism in the latter part of the twentieth century: Introduction. *Southern Review of Public Administration (pre-1986), 5*(3), 370.

Gitterman, A. (2004). Interactive andragogy: Principles, methods, and skills. *Journal of Teaching in Social Work, 24*(3-4), 95-112. doi: 10.1300/J067v24n03_07

Glaser, B. G., & Strauss, A. (1967). *The discovery of grounded theory: Strategies for qualitative research*. Mill Valley: Sociology Press.

Gonzalvo, P., Cañas, J. J., & Bajo, M.-T. (1994). Structural representations in knowledge acquisition. *Journal of Educational Psychology, 86*(4), 601-616.

Goucher, W. (2009). The challenge of security awareness training. *Computer Fraud & Security, 2009*(10), 15-16. doi: 10.1016/s1361-3723(09)70129-0

Griffith, I. L. (1997). *Drugs and security in the Caribbean: Sovereignty under siege*. University Park, PA: Pennsylvannia State University Press.

Griffiths, M., Brooks, D., & Corkill, J. (2011). *Defining the security professional: Definition through a body of knowledge*. SECAU Security Research Centre. Perth.

Guest, G., MacQueen, K. M., & Namey, E. E. (2012). *Applied thematic analysis*. Los Angeles: Sage Publications.

Hare, W., & Portelli, J. P. (1988). *Philosophy of education : Introductory readings*. Calgary: Detselig Enterprises.

Hilburn, T. B., Hirmanpour, I., Khajenoori, S., Turner, R., & Qasem, A. (1999). *A software engineering body of knowledge version 1.0*. Retrieved 11/03/2013, from http://www.sei.cmu.edu/reports/99tr004.pdf

Hirst, P. H. (1974). *Knowledge and the curriculum: A collection of philosophical papers*. London: Routledge.

Horrocks, I. (2001). Security training: Education for an emerging profession? *Computers & Security, 20*(3), 219-226. doi: 10.1016/s0167-4048(01)00306-6

Independent Commission Against Corruption NSW. (2013). *Investigation into allegations of corrupt conduct in the provision of security products and services by suppliers, installers and consultants*. Sydney: Author.

Inglehart, R. F., & Norris, P. (2012). The four horsemen of the apocalypse: Understanding human security. *Scandinavian Political Studies, 35*(1), 71-96. doi: 10.1111/j.1467-9477.2011.00281.x

International Foundation for Protection Officers. (2010). *The professional protection officer: Practical security strategies and emerging trends*. Burlington, MA Butterworth-Heinemann.

Jaques, E. (1989). *Requisite organization: The CEO's guide to creative structure and leadership*. Kingston, NY: Cason Hall.

Jinks, A. A. (1999). Applying education theory to nursing curricula: Nurse teachers' definitions of student centred andragogical teaching and learning concepts. *Journal of Further and Higher Education, 23*(2), 221-230. doi: 10.1080/0309877990230206

Johnson, A. G. (1995). *The Blackwell dictionary of sociology: A user's guide to sociological language*. Cambridge: Blackwell.

Johnson, B., & Christensen, L. (2004). *Educational research: Quantitative, qualitative, and mixed approaches* (2nd ed.). Boston: Pearson.

Johnston, R. (2003). Integrating methodologists into teams of substantive experts. *Studies in Intelligence, 47*(1), 57-65.

Johnston, R. G., & Warner, J. S. (2014). Is physical security a real field? *Journal of Physical Security, 7*(3), 13-15.

Kelly, A. V. (1982). *The curriculum: Theory and practice* (2nd ed.). London: Harper and Row.

Kelly, G. A. (1955). *The psychology of personal constructs*. New York: Norton.

Khairallah, M. (2006). *Physical security systems handbook: The design and implementation of electronic security systems*. Oxford: Elsevier/Butterworth-Heinemann.

Khan, M. E., & Manderson, L. (1992). Focus groups in tropical diseases research. *Health Policy and Planning, 7*(1), 56-66.

Kicinger, A. (2004). *International migration as a non-traditional security threat and the EU responses to this phenomenon*. Central European Forum for Migration Research Retrieved from www.cefmr.pan.pl.

Kiszelewska, A., & Coole, M. P. (2013). P*hysical security barrier selection: a decision support analysis.* Paper presented at the 6th Australian Security and Intelligence Conference, Perth.

Kline, E. H. (1981). To be a professional. *Southern Review of Public Administration, 5*(3), 258-281.

Knowles, M. S. (1980). The modern practice of adult education: From pedagogy to andragogy. Chicago: Follett

Kopala, M., & Suzuki, L. A. (1999). *Using qualitative methods in psychology*. Thousand Oaks: Sage.

Krebs, W. A., & Wilkes, G. A. (1981). *Collin's Australian Pocket Dictionary of the English Language*. Sydney: Collins

Krimsky, S., & Golding, D. (1992). *Social theories of risk*. Westport, Conn: Praeger.

Kruskal, J. B., & Wish, M. (1978). *Multidimensional scaling*. Newbury Park: Sage Publications.

Kumar, R. (1996). *Research methodology: A step-by step guide for beginners*. Melbourne: Longman.

Lab, S. P. (2014b). *Crime prevention: Approaches, practices and evaluations* (8th ed.). Waltham, MA: Elsevier.

LaFrance, M. (1997). Metaphors for human expertise: How knowledge engineers picture human expertise. In R. R. Hoffman, K. M. Ford & P. J. Feltovich (Eds.), *Expertise in context : Human and machine* (pp. 163-180). Menlo Park: AAAI Press.

Larson, M. S. (1977). *The rise of professionalism: A sociological analysis*. Berkeley: University of California Press.

Laycock, G. (2005). Defining crime science. In M. J. Smith & N. Tilley (Eds.), *Crime science: New approaches to preventing and detecting crime*. Portland: Willan.

Liamputtong, P., & Ezzy, D. (2006). *Qualitative research methods* (2nd ed.). New York: Oxford.

Lodahl, J. B., & Gordon, G. (1972). The structure of scientific fields and the functioning of university graduate departments. *American Sociological Review*, 37(1), 57-72.

Lussier, R. N. (2009). *Management fundamentals: Concepts, applications, skill development*. Mason: South-Western.

MacDonald-Ross, M. (1973). Behavioral objectives: A critical review. *Instructional Science, 2*, 1-52.

Mager, R. (1962). *Preparing instructional objectives*. Palo Alto, CA: Fearon Publisher.

Maher, C., & Burke, T. (1991). *Informed decision-making: The use of secondary data sources in policy studies*. Melbourne Longman Cheshire.

Makinda, S. M. (1998). Sovereignty and global security. *Security Dialogue, 29*(3), 281-292. doi: 10.1177/0967010698029003003

Malcolmson, J. (2009). *What is security culture? Does it differ in content from general organisational culture?* Paper presented at the International Carnahan Conference on Security Technology.

Manunta, G. (1997). *Towards a security science through a specific theory and methodology*. Doctor of Philosophy, University of Leicester.

Manunta, G. (1999). What is security? *Security Journal, 12*, 57-66.

Marewski, J. N., & Gigerenzer, G. (2012). Heuristic decision making in medicine. *Dialogues in Clinical Neuroscience, 14*(1), 77-89.

Marsh, C. J. (1986). *Curriculum: An analytical introduction*. Sydney: Ian Novak.

Marsh, C. J. (2004). *Key concepts for understanding curriculum* (4th ed.). London: Routledge Falmer.

Martin, C. S., & Guerin, D. A. (2005). *The interior design profession's body of knowledge*. Minneapolis: University of Minnesota.

Martin, D. W. (2000). *Doing psychology experiments* (5th ed.). Belmont: Wadsworth.

Marutello, F. (1981). The semantic definition of a profession. *Southern Review of Public Administration*, 246-257.

Maslow, A. H. (1970). *Motivation and personality*. New York: Harper & Row.

Maxwell, J. A. (1992). Understanding and validity in qualitative research. *Harvard Education Review, 62*(3), 279.

McAleese, R. (1999). Concept mapping-a critical review. *Innovations in Education and Training International, 36*(4), 351.

McCrie, R. D. (2004). The history of expertise in security management practice and litigation. *Security Journal, 17*(3), 11-19.

McLucas, A. C. (2003). *Decision making: Risk management, systems thinking and situation awareness*. Canberra: Argos Press.

McNeil, J. D. (1990). *Curriculum: A comprehensive introduction* (4th ed.). New York: HarperCollins.

McSweeney, B. (1999). *Security, identity, and interests: A sociology of international relations*. New York Cambridge University Press.

Michon, J. A. (1972). Multidimensional and hierarchical analysis of progress in learning. In L. W. Gregg (Ed.), *Cognition in Learning and Memory*. New York: Wiley

Miles, M. B., & Huberman, M. (1994). *Qualitative data analysis: An expanded sourcebook* (2nd ed.). Thousand Oaks: Sage Publications.

Mill, J. S. (1910). *Utilitarianism, liberty, representative government*. London: JM Dent and Sons.

Misiuk, A. (2011). Deliberations on security. *Internal Security, 3*(2), 255-266.

Morris, P. W. G., Crawford, L., Hodgson, D., Shepherd, M. M., & Thomas, J. (2006). Exploring the role of formal bodies of knowledge in defining a profession – the case of project management. *International Journal of Project Management, 24*(8), 710-721. doi: 10.1016/j.ijproman.2006.09.012

Mosher, F. C. (1968). *Democracy and the public service*. New York: Oxford University Press.

Nalla, M., & Morash, M. (2002). Assessing the scope of corporate security: Common practices and relationships with other business functions. *Security Journal, 15*, 7–19.

Nef, J. (1999). *Human security and mutual vulnerability: The global political economy of development and underdevelopment*. Ottawa: International Development Research Centre.

Neocleous, M. (2007). Security, commodity, fetishism. *Critique, 35*(3), 339-355. doi: 10.1080/03017600701676738

Norman, T. (2007). *Integrated security systems design: Concepts, specifications, and implementation*. Boston, MA: Elsevier Butterworth-Heinemann.

Norman, T. L. (2012). *Electronic access control*. Oxford: Elsevier.

Novak, J. D. (1993). Human constructivism: a unification of psychological and epistemological phenomena in meaning making. I*nternational Journal of Personal Construct Psychology, 6*, 167-193.

O'Block, R. L., Donnermeyer, J. F., & Doeren, S. E. (1991). *Security and crime prevention* (2nd ed.). Boston: Butterworth-Heinemann.

O'Shea, L. S., & Awwad-Rafferty, R. (2009). *Design and security in the built environment*. New York: Fairchild Books.

Olufs, D. W. (1985). The limits of professionalism. *Public Administration Quarterly*, 26-46.

Ornstein, A. C., & Hunkins, F. P. (1988). *Curriculum: Foundations, principles, and issues*. Englewood Cliffs, N.J.: Prentice-Hall.

Paris, R. (2001). Human security: Paradigm shift or hot air? *International Security, 26*(2), 87-102. doi: 10.1162/016228801753191141

Parker, M. (Ed.). (2007). *Dynamic security: The democratic therapeutic community in prison*. London: Jessica Kingsley.

Patel, V. L., & Ramoni, M. F. (1997). Cognitive models of directional inference in expert medical reasoning. In R. R. Hoffman, K. M. Ford & P. J. Feltovich (Eds.), *Expertise in context: Human and machine* (pp. 67-99). Menlo Park: AAAI Press.

Pearson, R. L. (2007). *Electronic security systems: A manager's guide to evaluating and selecting system solutions*. Boston: Butterworth-Heinemann.

Peterson, K. L. (2014). The politics of corporate security and the translation of national security. In K. Walby & R. K. Lippert (Eds.), *Corporate security in the 21st century: Theory and practice in international perspective* (pp. 78-94). Basingstoke: Palgrave Macmillan.

Phinney, C., & Smith, C. L. (2009). Security education in Singapore: A study of knowledge structures in electronic security technology. *Security Journal, 24*, 133-148.

Piá, A. B., Blasco-Tamarit, E., & Muñoz-Portero, M. J. (2011). Different applications of concept maps in higher education. *Journal of Industrial Engineering and Management, 4*(1), 81-102. doi: 10.3926/jiem.2011.v4n1.p81-102

Piaget, J. (1951). *Psychology of intelligence*. London: Routledge.

Pion-Berlin, D. (2010). Neither military nor police: Facing heterodox security challengers and filling the security gap in democratic Latin America. *Democracy and Security, 6*(2), 109-127. doi: 10.1080/17419161003715710

Posner, G. J., & Rudnitsky., A. N. (1982). *Course design: A guide to curriculum development for teachers* (2nd ed.). New York: Longman.

Prenzler, T. (2005). Mapping the Australian security industry. *Security Journal, 18*(4), 51-64. doi: 10.1057/palgrave.sj.8340211

Prenzler, T., Earle, K., & Sarre, R. (2009). Private security in Australia: Trends and key characteristics. *Trends & Issues in Crime and Criminal Justice*, 374.

Prenzler, T. J., & Sarre, R. (1998). *Regulating private security in Australia*. Canberra: Australian Institute of Criminology.

Prenzler, T. J., & Sarre, R. (2012). The evolution of security industry regulation in Australia: A critique. *International Journal for Crime and Justice, 1*(1), 38-51.

Rakshit, S., & Ananthasuresh, G. K. (2007). An amino acid map of inter-residue contact energies using metric multi-dimensional scaling. *Journal of Theoretical Biology, 250*, 291-297.

Reveron, D. S., & Mahoney-Norris, K. A. (2011). *Human security in a borderless world*. Philadelphia, PA: Westview Press.

Richardson, A. J. (1988). Accounting knowledge and professional privilege. *Accounting, Organizations and Society, 13*(4), 381-396. doi: 10.1016/0361-3682(88)90012-8

Roe, P. (2008). The 'value' of positive security. *Review of International Studies, 34*(4), 777-794. doi: 10.1017/s0260210508008279

Rogers, B. (2000). Personal opinion: A framework for higher education in the security field. Security Journal, 13, 65-68.

Rogers, B., Palmgren, D., Giever, D., & Garcia, M. L. (2007). *Security education in the 21st century: The role of engineering*. American Society for Engineering Education.

Roper, C. A. (1997). *Physical security and the inspection process*. Boston: Butterworth-Heinemann.

Rothschild, E. (1995). What is security? *Daedalus, 124*(3), 53-98.

Rundblad, G. (2006). *Recruiting a representative sample*. Retrieved May 20, 2010, from www.appliedlinguistics.org.uk

Sarre, R., & Prenzler, T. (2009). *The law of private security in Australia* (2nd ed.). Pyrmont: Thomson Reuters.

Schensul, J. J., LeCompte, M. D., Nastasi, B. K., & Borgatti, S. P. (1999). *Enhanced ethnographic methods: Audiovisual techniques, focused group interviews, and elicitation*, (Ethnographers tool kit, Vol. 3). Walnut Creek, CA.

Schiffman, S. S., Reynolds, M. L., & Young, F. W. (1981). *Introduction to multidimensional scaling: Theory, methods, and applications*. New York: Academic Press.

Schnabolk, C. (1983). *Physical security: Practices and technology*. Boston: Butterworths.

Seidl, D. (2004). *Luhmann's theory of autopoietic social systems*. Munich Business Research, 2.

Sennewald, C. A. (2013). *Security consulting* (4th ed.). Waltham, MA: Butterworth-Heinemann.

Shah, A. K., & Oppenheimer, D. M. (2008). Heuristics made easy: An effort-reduction framework. *Psychological Bulletin, 134*(2), 207.

Shepard, R. N., Romney, A. K., & Nerlove, S. B. (Eds.). (1972). *Multidimensional scaling: Theory and applications in the behavioral sciences*. New York: Seminar Press.

Silverman, D. (2002). *Doing qualitative research: A practical handbook*. London: Sage Publications.

Simon, H. A., & Chase, W. G. (1973). Skill in chess: Experiments with chess-playing tasks and computer simulation of skilled performance throw light on some human perceptual and memory processes. *American Scientist, 61*(4), 394-403.

Smart, J. P., & Pontifex, M. R. (1993). Human resources management and the Australian Human Resources Institute: The profession and its professional body. *Asia Pacific Journal of Human Resources, 31*(1), 1-19. doi: 10.1177/103841119303100102

Smith, C. L. (2002). *A method for understanding students' perceptions of concepts in the defence in depth strategy*. Paper presented at the 3rd Australian Information Warfare and Security Conference 2002, Perth.

Smith, C. L., & Brooks, D. J. (2013). *Security science: The theory and practice of security*. Amsterdam: Elsevier.

Somerson, I. S. (2009). *The art and science of security risk assessment*. Alexandria, VA: ASIS International.

Spradley, J. P. (1979). *The ethnographic interview*. New York Holt, Rinehart, and Winston.

Stake, R. E. (2010). *Qualitative research: Studying how things work*. New York: Guildford Press.

Sternberg, R. J. (1997). Cognitive conceptions of expertise. In R. R. Hoffman, K. M. Ford & P. J. Feltovich (Eds.), *Expertise in context: Human and machine* (pp. 149-162). Menlo Park: AAAI Press.

Stone, M. (2009). *Security according to Buzan: A comprehensive security analysis*. Security Discussion Paper Series.

Talbot, J., & Jakeman, M. (2009). *Guide to SRMBOK physical security specifications and postures*. Canberra: Jakeman Business Solutions.

Talbot, J., & Jakeman, M. (2009). *Security risk management body of knowledge*. New Jersey: John Wiley & Sons.

Tashakkori, A., & Teddlie, C. (1998). *Mixed methodology: Combining qualitative and quantitative approaches*. Thousand Oaks, Calif.: Sage.

Tooma, M. (2008). *Safety, security, health and environment law*. Leichhardt, NSW: Federation Press.

Tooma, M. (2011). S*afety, security, health and environment law* (2nd ed.). Annandale, N.S.W.: Federation Press.

Toombs, W. E., & Tierney, W. G. (1993). Curriculum definitions and reference points, *Journal of Curriculum and Supervision, 8*(3), 175-195).

Tovey, M. D., & Lawlor, D. R. (2004). *Training in Australia: Design, delivery, evaluation, management* (2nd ed.). Sydney: Pearson Education Australia.

Tyler, R. W. (1949). *Basic principles of curriculum and instruction*. Chicago: University of Chicago Press.

Tynjälä, P. (1999). Towards expert knowledge? A comparison between a constructivist and a traditional learning environment in the university. *International Journal of Educational Research, 31*(5), 357-442.

Ullman, R. H. (1983). Redefining security. *International Security, 8*(1), 129-153.

Underwood, G. (1984). *The security of buildings*. London: Butterworths.

United Nations. (1986). *Concepts of security*. New York: United Nations.

von Glasersfeld, E. (1982). An interpretation of Piaget's constructivism. *Revue Internationale de Philosophie, 36*(4), 612-635.

Walker, P. (1998). *Electronic security systems: Reducing false alarms* (3rd ed.). Oxford: Newnes.

Walsh, T. J., & Healy, R. J. (2012). *Protection of assets: Physical security*. Alexandria, VA: ASIS International.

Wang, Y. (2005). *Defining non-traditional security and its implications for China*. Beijing: Institute of World Economics and Politics, Chinese Academy of Social Sciences.

Wilensky, H. L. (1964). The professionalisation of everyone? *American Journal of Sociology, 70*(2), 137-158.

Wilson, J., & Oyola-Yemaiel, A. (2001). The evolution of emergency management and the advancement towards a profession in the United States and Florida. *Safety Science, 39*(1), 117-131. doi: 10.1016/s0925-7535(01)00031-5

Wolfers, A. (1952). "National security" as an ambiguous symbol. *Political Science Quarterly, 67*(4), 481-502.

Yanay, U. (2006). Personal security and the 'right' to protection. *Social Policy & Administration, 40*(5), 509-525. doi: 10.1111/j.1467-9515.2006.00502.x

Zeitz, C. M. (1997). Some concrete advantages of abstraction: How experts' representations faciliate reasoning. In R. R. Hoffman, K. M. Ford & P. J. Feltovich (Eds.), *Expertise in context: Human and machine* (pp. 43-65). Menlo Park: AAAI Press.

Zender, L. (2009). *Security: Key ideas in criminology*. Paris: Lavoiser.

Zietek, A. (2008). Migration as a security challenge facing Europe. *Revista Universitaria Europea*, 101-122.

Zipser, B. (1999). Professionals and the standard of care. *Torts Law Journal, 7*(2), 167.

Appendix A

PILOT STUDY PHASE TWO INTERVIEW QUESTIONNAIRE

Curtin University
School of Science and Mathematics Education Centre

Participant Information Letter: Semi-structured Interview Research Questionnaire Invitation

This research study is being undertaken as part of the requirements towards the award of Doctor of Philosophy (PhD) of Science and Mathematics Education at Curtin University in Western Australia.

Aim: To undertake a cultural domain analysis to identify a formal knowledge system (body of knowledge) for the domain of physical Security.

Guidelines: This phase of the research enquiry is employing a semi-structured interview questionnaire. The purpose of the interview and questionnaire is to to draw out implicit knowledge concepts relating to physical security's body of knowledge, which are not presented in the reviewed text, yet considered valuable by experts such as yourself. As such, the core aspects of your role within this study will consist of providing experience-based knowledge in response to specific interview questions that relate to uncovering physical security's knowledge concepts and subordinate concepts.

Risks and Discomforts: There are no foreseeable risks or discomforts associated with your participation in this study. However, you are requested to provide an hour of your time and be willing to have the interview recorded to enhance analysis and for reliability validity purposes.

Confidentiality: Information obtained from this study that could identify you will be kept private to the extent allowed by law. The information you provide will be kept separate from your personal details and only I and research supervisors will have access to this. The interview transcript will not have your name or any other identifying information on it and in adherence with university policy, the interview tapes and transcribed information will be kept in a locked cabinet for at least five years, before a decision is made as to whether it should be destroyed.

Consent to Participate: Your involvement in this study is entirely voluntary and you have the right to withdraw at any stage without affecting your rights or my responsibilities. Once you have signed the consent form, it will be acknowledged that you have agreed to participate and allow me to use your data in this research.

Further Information

This study has been approved by Curtin University's Human Research Ethics Committee (Approval Number SMEC-10-13, 2013). The Committee is comprised of members of the public, academics, lawyers, doctors and pastoral carers. If needed, verification of approval can be obtained either by writing to the Curtin University Human Research Ethics Committee, c/- Office of Research and Development, Curtin University, GPO Box U1987, Perth, 6845 or by telephoning 9266 2784 or by emailing hrec@curtin.edu.au

If you would like further information about the study, please contact myself Michael Coole; 08 63045123, or email: m.coole@ecu.edu.au or,
Professor David Treagust; 08 92667924, or email: D.Treagust@curtin.edu.au or,
Dr Dave Brooks; 08 63042827, or email: d.brooks@ecu.edu.au

Study Consent Form

Thank you for choosing to participate in this research study, please read the terms of informed consent below.

- I understand the purpose and procedure of the study.
- I have been provided with the participation information sheet.
- I understand that the procedure itself may not benefit me.
- I understand that my involvement is voluntary and I can withdraw at any time without a problem.
- I understand that no personal identifying information such as name and address will be used in any published materials.
- Í understand that all information will be securely stored for at least 5 years before a decision is made as to whether it should be destroyed.
- I have been given the opportunity to ask questions about this research.

Your signature below indicates that you consent to participate in this study.

I_____ agree to participate in this research study. In line with the requirements of informed consent, I provide my consent.

Signature_____ Date_____/____/____.

This document was witnessed by Michael Coole_____
Date____/___/____.

Semi-structured Interview Research Questionnaire

Phase one of the study extracted through literature critique physical security knowledge concepts and subordinate concepts. These were subjected to a numerical analysis highlighting the top 49 thematic knowledge concepts and subordinate concepts resulting in a combined knowledge table. Tabulated data was then subjected to a deductive analysis where their inclusion as a concept and their relation with other concepts and subordinate concepts were graphically mapped presenting linkages.

1) The table shows the literature extractions top 49 thematic knowledge categories and subordinate concepts. This table was produced through the synergizing of three text's salient knowledge categories and subordinate concepts. This required a number of synonymous terms to be combined towards producing a phase table of knowledge categories and subordinate concepts. Could you please indicate your agreement/acceptance or disagreement of the following combined terms?

    a) Threat, threat definition and threats were combined to produce the thematic category of Threat.
    b) Entry control/access control was combined with Entry/Access control, entrances and access delay to produce the thematic theme of Entry control.
    c) Analysis, analysis and evaluation, and EASI model an analysis and evaluation approaches were combined to produce the theme Analysis and evaluation.
    d) Closed circuit television (CCTV) was combined with closed-circuit television/CCTV and closed circuit television-CCTV to produce the theme Closed circuit television (CCTV).
    e) The Facility was combined with Facility characterization to produce the thematic theme Facility characterization.
    f) Neutralization, use of force and arrest were combined to produce the thematic category of Use of force.
    g) Legal issues were combined with law to produce the thematic category of Law.
    h) Traffic controls and Traffic were combined to produce the thematic category of Traffic control.
    i) Theft controls was combined with loss prevention a term used to refer to theft prevention to produce the thematic category of Loss prevention.
    j) Detection a salient theme was combined with alarm systems, another salient theme to produce the category of Detection systems.
    k) Safes and vaults as a thematic category were combined with safes to produce the category of Safes and vaults.
    l) The thematic category of investigations was excluded from the table as it relates to management practices rather than the diagnosis, inference and treatment of security or loss coupled threat concerns.

2) Within these knowledge categories are some physical security themes that are unambiguous in what they represent. However, there are some themes representing more ambiguous term, can you please tell me what you believe the following themes represent in terms of knowledge required for physical security professionals?

a) Analysis and evaluation
b) System
c) Facility characterization
d) Terrorism
e) Crimes
f) Traffic controls
g) Security principles
h) Drugs

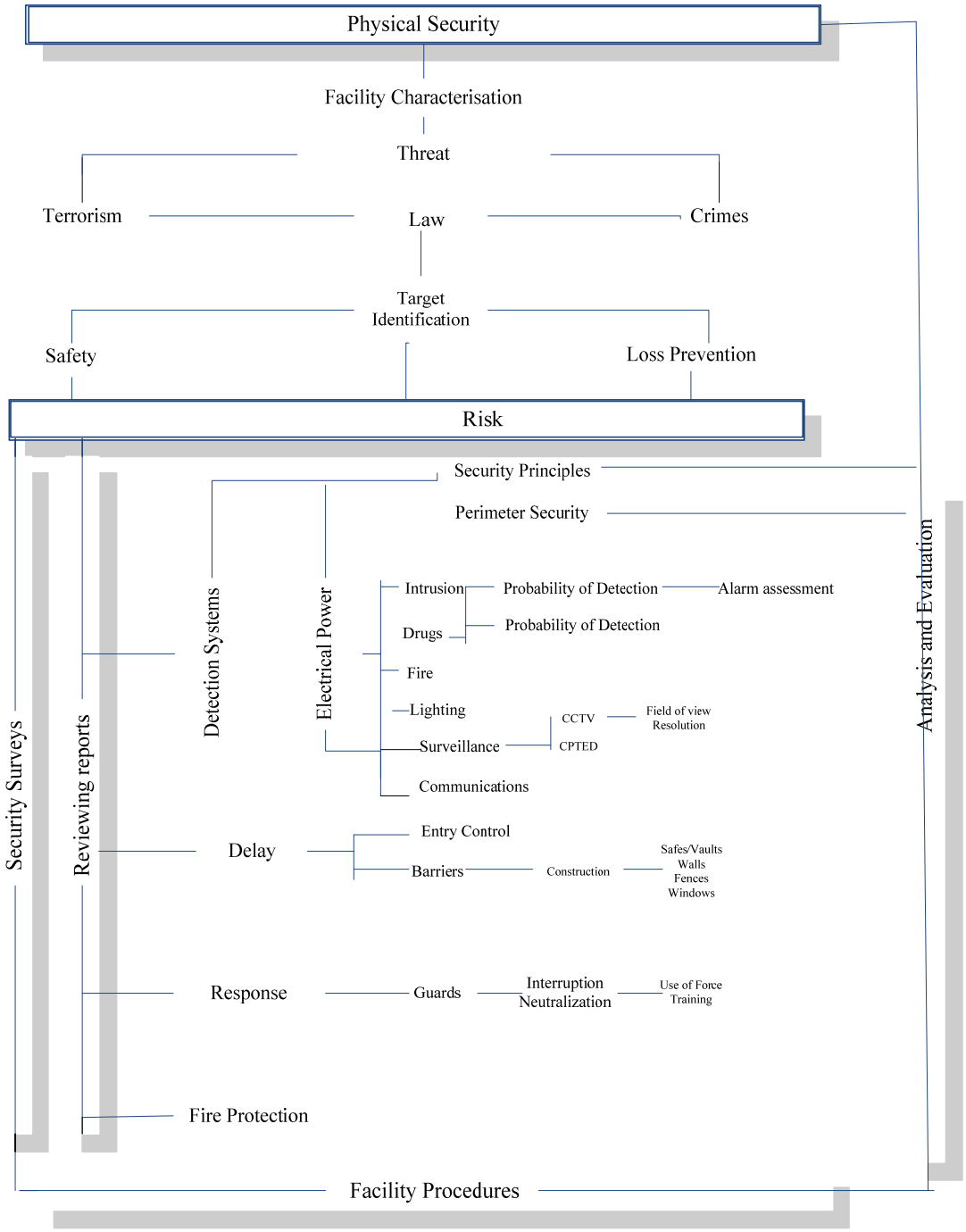
3) This table lists the salient 49 knowledge concepts and subordinate concepts for physical security's body of knowledge, do you agree with these?
4) Do you believe any of the knowledge concepts and subordinate concepts should be removed and why?
5) The top 49 knowledge categories have been organised into a hierarchical concept map to illustrate both the structure of physical security's body of knowledge including core and supporting concepts and their relations. This map aims to highlight the knowledge and structure of physical security's knowledge base towards the diagnosis, inference and treatment of security or loss coupled threat concerns manifested through unlawful access and/or crime enablers towards the protection of assets including people, information and property. Do you support this overall goal for physical security, and based on this goal do you support the structure of this map?
6) Do you believe the whole structure captures the ideas underlying physical security?
7) Do you feel that any of the knowledge concepts or subordinate concepts needs relocating and why?
8) From your knowledge of physical security, do you believe that the table and knowledge map captures the knowledge requirements for a physical security professional, and if not, what knowledge concepts and subordinate concepts are missing and why?
9) What do you feel are the three most important knowledge concepts for physical security?
10) The methodology drew on a 7 × 7 matrix to identify, categories and present core and subordinate knowledge themes and concepts resulting in the top 49. Do you believe this is sufficient or do you feel this would be best expanded to a 9 × 9 matrix to capture further subordinate knowledge concepts?
11) Do you have any further comments to enhance the tabulated knowledge categories and subordinate concepts, the heuristic map or methodology to enhance the study?

Table 1 Pilot study: Phase 1 combined texts knowledge category data

Physical Security						
Security	Threat	Detection systems	System	Response	Delay	Analysis and Evaluation
Fire protection	Law	Doors	Locks	Surveillance	Facility characterization	Closed circuit television (CCTV)
Entry Control/Access control	Risk	Lighting	Barriers	Windows	Walls	Facility procedures
Terrorism	Target identification	Fences	Loss prevention	Communications	Use of force	Alarm assessment
Electric power	Reviewing reports	Perimeter security	Security surveys	Safety	Crimes	Traffic control
Training	Intrusion detection	Interruption	Safes and vaults	CPTED	Guards	Glass
Field of view	Construction	Risk assessment	Resolution	Probability of detection	Security principles	Drugs

Table 2 Pilot study: Phase 1 hierarchical taxonomic table of knowledge category themes, concepts, subordinate concepts and their elements (Adjusted from Spradley (1979, p. 137).

Security								
Facility Characterization								Analysis & Evaluation
Threat								
Terrorism			Law			Crimes		
Target identification								
Safety						Loss Prevention		
Risk								
Security Surveys	Reviewing Reports	Detection Systems	Electric Power	Security Principles				
				Perimeter Security				
				Intrusion	Probability Detection	Alarm assessment		
				Drugs	Probability Detection			
				Fire				
				Lighting				
				Surveillance	CCTV	Field of View		
						Resolution		
					CPTED			
				Communications				
		Delay			Entry Control	CPTED		
						Locks		
						Doors		
					Barriers	Construction	Safes/Vaults	
							Walls	
							Fences	
							Glass	
							Windows	
		Response			Guards			
						Interruption		
							Use of Force	
						Neutralization	Training	
		Fire Protection						
		Facility Procedures						


Physical Security
Facility Characterisation
Threat
Terrorism
Law
Crimes
Target Identification
Safety
Loss Prevention
Risk
Security Principles
Perimeter Security
Detection Systems
Electrical Power
Intrusion
Probability of Detection
Alarm assessment
Drugs
Probability of Detection
Fire
Lighting
Surveillance
CCTV
CPTED
Field of view
Resolution
Communications
Delay
Entry Control
Barriers
Construction
Safes/Vaults
Walls
Fences
Windows
Response
Guards
Interruption
Neutralization
Use of Force
Training
Fire Protection
Security Surveys
Reviewing reports
Analysis and Evaluation
Facility Procedures

Appendix B

PILOT STUDY MDS SURVEY QUESTIONNAIRE

Phase Three Multidimensional Statistical Scaling Survey Questionnaire (Page 1)

When compared to			Similar	1	2	3	4	5	6	7	8	9	10	Dissimilar
Security		Law												
Security		Facility contextualization												
Security		Threat												
Security		Risk												
Security		Planning & Design												
Security		Infrastructure												
Security		Analysis & evaluation												
Security		Systems theory												
Security		Security theory & principles												
Security		Defence in depth												
Security		Crime prevention theory												
Security		Communications skills												
Security		Detection												
Security		Delay												
Security		Response												
Security		Structural strengths												
Security		Barriers												
Security		Lighting												
Security		Surveillance												
Security		Door furniture												
Security		Safes & vaults												
Security		Movement control												
Security		Electrical power												
Security		Entry control												
Security		Detection systems												
Security		Fire protection												
Security		Reviewing reports												
Security		CCTV												
Security		Target identification												
Law		Security												
Law		Facility contextualization												
Law		Threat												
Law		Risk												
Law		Planning & Design												
Law		Infrastructure												
Law		Analysis & evaluation												

Appendix C

PILOT STUDY PHASE FOUR FOCUS GROUP SEMI-STRUCTURED QUESTIONNAIRE

Phase 4 Focus Group Semi-Structured Interview Questionnaire

The jurisdictional focus for Physical Security is directed towards the diagnosis, inference and treatment of security or loss coupled risk concerns associated with people, information and property manifested through unlawful access plus crime enablers in the protection of assets. Such treatment results in a security function as an organised complex of specialised technological, physical and procedural elements integrated into a protective barrier system.

Phases One and Two provided propositional maps (Figures 1 & 2) for understanding the knowledge domain of physical security. These maps have drawn out a vast number of theories, knowledge concepts and subordinate concepts from the domain of physical security. One map (Figure 1) is derived from a qualitative analysis showing local connections, and the second a broader map (Figure 2) established through perceived ratings of similarity and dissimilarity showing macro structure organised according to clusters of knowledge relating to the professional dimensions of practice.

Curriculum development entails the identification, selection and organisation of a set of intended learning outcomes. This should be based on educational goals in terms of what is to be learned. The goals indicate why it is to be learned (Posner & Rudnitsky, 1982, p. 8)

Phase 3 Research Question: What are the learning objectives and knowledge requisites for physical security professionals?

Key points: The reviewed literature highlighted a number of salient points for professional education:

a) The need to consider the broader goals;
b) Units should be planned in context with other units-relationships;
c) Sequence-planned, where units both precede and follow other learning units;
d) Should teach the science or knowledge that the domain is built;
e) Learning of principles and attitudes;
f) General graduate attributes;
g) Content- scope- organisation-sequence.

Accordant with these key points, Eraut (1994, p. 119) highlights three key questions for every profession:

A. What is the professional knowledge base?

B. What is best learned in higher education?
C. What is best learned in professional practice, and what is best learned through an integrated course involving both contexts?
D. What has to be learned before qualification, and what is best postponed until after qualification?

Interview Questions:

1. What is the higher education learning objective/s for a physical security professional?

2. In terms of articulating a formal knowledge system, based on these maps what do you see as the foundation content requirements to be learned by physical security professionals before qualification?

3. Higher education students should learn or know the science or knowledge of which their future domain is built. Based on this view, what is the scope of higher education knowledge?

4. How should these units be organized?

5. Do you believe these maps capture the knowledge concepts required for a physical security professional?

6. What are the strengths and perhaps weaknesses of these maps in terms of establishing a physical security professional's knowledge system?

Appendix D

PHASE TWO SEMI-STRUCTURED INTERVIEW QUESTIONNAIRE

Curtin University
School of Science and Mathematics Education Centre

Participant Information Letter: Semi-structured Interview Research Questionnaire Invitation

This research study is being undertaken as part of the requirements towards the award of Doctor of Philosophy (PhD) of Science and Mathematics Education at Curtin University in Western Australia.

Aim: To undertake a cultural domain analysis to identify a formal knowledge system (body of knowledge) for the domain of physical Security.

Guidelines: This phase of the research enquiry is employing a semi-structured interview questionnaire. The purpose of the interview and questionnaire is to to draw out implicit knowledge concepts relating to physical security's body of knowledge, which are not presented in the reviewed text, yet considered valuable by experts such as yourself. As such, the core aspects of your role within this study will consist of providing experience-based knowledge in response to specific interview questions that relate to uncovering physical security's knowledge concepts and subordinate concepts.

Risks and Discomforts: There are no foreseeable risks or discomforts associated with your participation in this study. However, you are requested to provide an hour of your time and be willing to have the interview recorded to enhance analysis and for reliability validity purposes.

Confidentiality: Information obtained from this study that could identify you will be kept private to the extent allowed by law. The information you provide will be kept separate from your personal details and only I and research supervisors will have access to this. The interview transcript will not have your name or any other identifying information on it and in adherence with university policy, the interview tapes and transcribed information will be kept in a locked cabinet for at least five years, before a decision is made as to whether it should be destroyed.

Consent to Participate: Your involvement in this study is entirely voluntary and you have the right to withdraw at any stage without affecting your rights or my responsibilities. Once you have signed the consent form, it will be acknowledged that you have agreed to participate and allow me to use your data in this research.

Further Information
This study has been approved by Curtin University's Human Research Ethics Committee (Approval Number SMEC-10-13, 2013). The Committee is comprised of members of the public, academics, lawyers, doctors and pastoral carers. If needed, verification of approval can be obtained either by writing to the Curtin University

Human Research Ethics Committee, c/- Office of Research and Development, Curtin University, GPO Box U1987, Perth, 6845 or by telephoning 9266 2784 or by emailing hrec@curtin.edu.au

If you would like further information about the study, please contact myself Michael Coole; 08 63045123, or email: m.coole@ecu.edu.au or,
Professor David Treagust; 08 92667924, or email: D.Treagust@curtin.edu.au or,
Dr Dave Brooks; 08 63042827, or email: d.brooks@ecu.edu.au

Study Consent Form

Thank you for choosing to participate in this research study, please read the terms of informed consent below.

- I understand the purpose and procedure of the study.
- I have been provided with the participation information sheet.
- I understand that the procedure itself may not benefit me.
- I understand that my involvement is voluntary and I can withdraw at any time without a problem.
- I understand that no personal identifying information such as name and address will be used in any published materials.
- Í understand that all information will be securely stored for at least 5 years before a decision is made as to whether it should be destroyed.
- I have been given the opportunity to ask questions about this research.

Your signature below indicates that you consent to participate in this study.

I_____ agree to participate in this research study. In line with the requirements of informed consent, I provide my consent.

Signature_____ Date_____/____/____.

This document was witnessed by Michael Coole_____
Date____/___/____.

Semi-structured Interview Research Questionnaire

Phase (a) one of the study extracted through literature critique physical security knowledge concepts and subordinate concepts. These were subjected to a numerical analysis highlighting the top 49 thematic knowledge concepts and subordinate concepts resulting in a combined knowledge table. Tabulated data was then subjected to a deductive analysis where their inclusion as a concept and their relation with other concepts and subordinate concepts were graphically mapped presenting linkages.

1) The table shows the literature extractions top 49 thematic knowledge categories and subordinate concepts. This table was produced through the synergizing of 15 text's salient knowledge categories and subordinate concepts. Is there any knowledge category concepts you would like clarified before we begin? Could you please indicate your support or disagreement with these terms and what you believe the category should be labelled?

2) The knowledge table lists the 49 salient extracted knowledge concepts and subordinate concepts for physical security's body of knowledge, do you agree with these, and if not, what knowledge concepts and subordinate concepts are missing and why?

3) Do you believe any of the knowledge concepts and subordinate concepts should be removed and why?

4) The top 49 knowledge categories have been organised into a hierarchical concept map to illustrate both the structure of physical security's body of knowledge including core and supporting concepts and their relations. This map aims to highlight the knowledge and structure of physical security's knowledge base towards the diagnosis, inference and treatment of security or loss coupled threat concerns. Do you support the structure of this map based on the overall goal for physical security?

5) Do you feel that any of the knowledge concepts or subordinate concepts needs relocating and why?

6) What do you feel are the three most important knowledge concepts for physical security?

Table 1: carried forward knowledge concept categories.

Physical Security			
Door Furniture	Defence in Depth	Situational crime Prevention	Infrastructure
Structural Strengths	Safes & Vaults	Electric Power	Delay
Surveillance	Windows	Glass	Walls
Drugs	Interruption	Field of View	Security Surveys
Movement control			

Table 2: Phase 1 combined text knowledge category data.

Physical Security						
Security	System	CCTV	People	Control	Access control	Planning & design
Alarms	Facility contextualization	Doors	Crime	Building	Risk	Data & Information
Lighting	Threat	Sensors	Detection	Response	Locks	Assets
Device	Lenses	Analysis & evaluation	Technology	Emergency	Costs	Attack
Standards	Keys	Reports	Safety	Equipment	Fire	CPTED
Network	Barriers	Procedures	Fencing	Prevention	Loss	Adversary
Property	Terrorism	Guard	Law	Door furniture	Defence in depth	Situational crime prev
Infrastructure	Structural strengths	Safes & vaults	Electric power	Delay	Surveillance	Windows
Glass	Walls	Drugs	Interruption	Field of view	Security surveys	Security theory & principles
Movement control						

Table 3: Phase 1qualitative hierarchical knowledge concept category table.

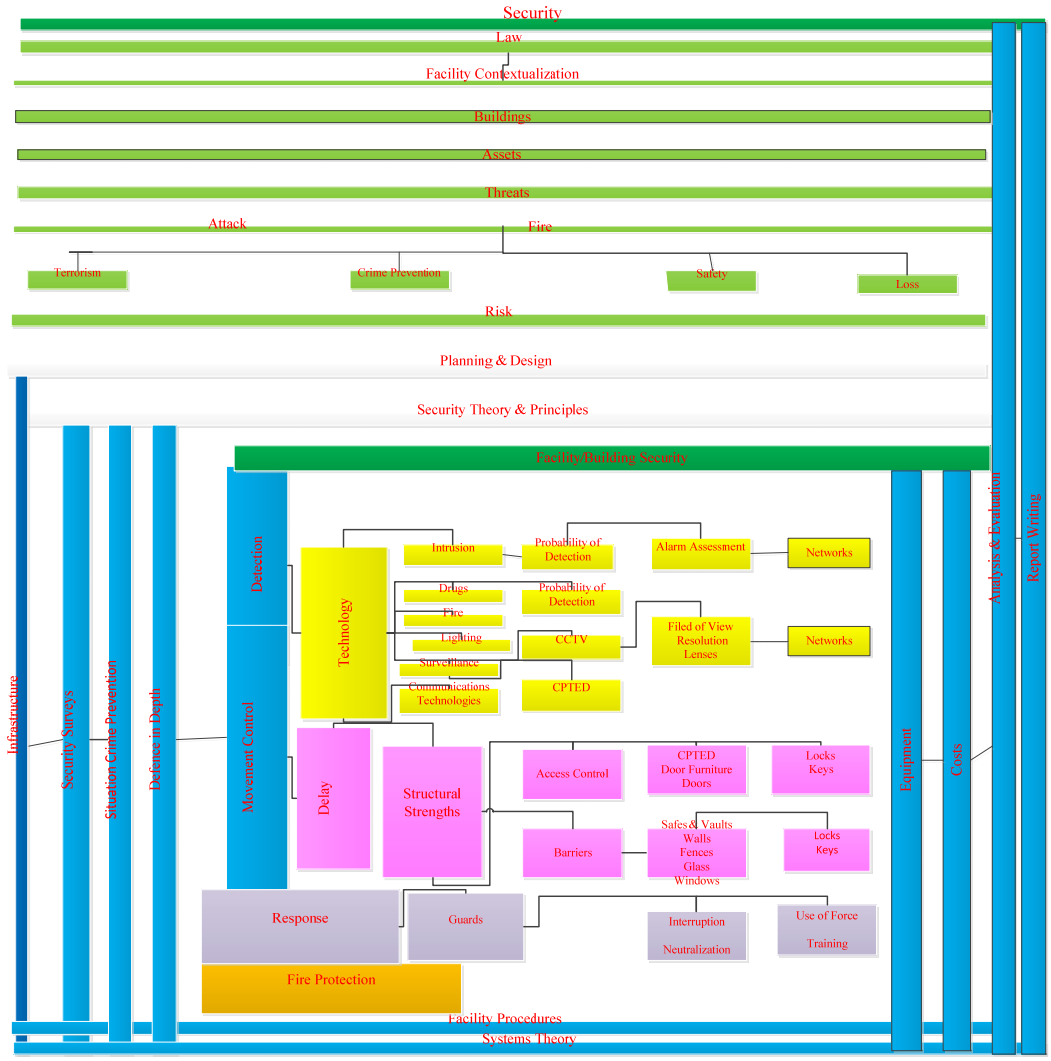
Security			
Law			
Facility Contextualization			
Buildings			
Assets			
Threats			
Attack			Fire
Adversary			
Terrorism	Crime	Safety	Loss
Risk			
Prevention			
Planning & Design			
Security Theories & Principles			

Infrastructure	Security Surveys	Situational Crime Prevention	Defence in Depth	Detection	Electrical Power	Technology	Equipment	Costs	Analysis & Evaluation	Report writing

Facility/Building Security			
Intrusion	Probability Detect	Alarm assess	Networks
Drugs	Probability Detect		
Fire			Networks
Lighting			
Surveillance	CCTV	Field of View	Lenses
			Resolution
	CPTED		
Communications	Networks		
Technologies			

Movement control				
Delay	Structural strengths	Access Control	CPTED	
			Door furniture	Locks
			Doors	Keys
		Barriers	Safes/Vaults	
			Walls	
			Fences	
			Glass	
			Windows	Locks
Response		Guards		
			Interruption	
			Neutralization	
Emergency				
Facility Procedures				
Systems Theory				

Figure 1 Phase 1structural heuristic.



End of Questionnaire

Thank you for your participation and time.

Appendix E

PHASE 3 MDS SURVEY QUESTIONNAIRE

Participant Information Letter: Multidimensional Statistical Scaling Survey Questionnaire Invitation

My name is Michael Coole, I am currently undertaking a PhD through Curtin University, Western Australia, to highlight and map Physical Security's knowledge system. Occupational domains are structurally understood through the similarity and contrast between their knowledge categories. The study is using a mathematical process to map the structure of Physical Security knowledge category concepts utilizing two survey questionnaires. As participants open the link you will be randomly assigned one of two surveys to complete.

Aim: To uncover a knowledge structure for physical Security through a cultural domain analysis.

Guidelines: As a security professional it is requested that you spend approximately 15 minutes completing the linked survey. The survey contains a rating scale questionnaire seeking your perceived relationship between matched pairs of physical security concepts. I would like you to score in the questionnaire boxes your perceived degree of difference where 1 indicates the knowledge concepts are Highly Similar and 10 indicates they are Dissimilar.

If you have any questions please contact Michael Coole:
Michael.coole@student.curtin.edu.au

Follow this link to the Survey:

https://curtin.asia.qualtrics.com/SE/?SID=SV_e5wGURy06vh0KAl

Multidimensional Statistical Scaling Survey Questionnaire

When compared to			Similar	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	Dissimilar
Security		Threat												
Security		Context												
Security		Security planning & design												
Security		Environmental conditions												
Security		CPTED												
Security		Defence in depth												
Security		Movement control												
Security		Surveillance												
Security		Detection												
Security		Technology												
Security		Lighting												
Security		Sensors												
Security		CCTV												
Security		Delay												
Security		Structural strength												
Security		Barriers												
Security		Security containers												
Security		Locks/cylinders												
Security		Response												
Security		Professional practice												
Security		Engineering design process												
Security		Analysis & evaluation												
Security		Situational crime prevention												
When compared to				**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	
Threat		Context												
Threat		Security planning & design												
Threat		Environmental conditions												
Threat		CPTED												
Threat		Defence in depth												
Threat		Movement control												
Threat		Surveillance												
Threat		Detection												
Threat		Technology												

Threat		Lighting												
Threat		Sensors												
Threat		CCTV												
Threat		Delay												
Threat		Structural strength												
Threat		Barriers												
Threat		Security containers												
Threat		Locks/cylinders												
Threat		Response												
Threat		Professional practice												
Threat		Engineering design process												
Threat		Analysis & evaluation												
Threat		Situational crime prevention												
When compared to				**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	
Context		Security planning & design												
Context		Environmental conditions												
Context		CPTED												
Context		Defence in depth												
Context		Movement control												
Context		Surveillance												
Context		Detection												
Context		Technology												
Context		Lighting												
Context		Sensors												
Context		CCTV												
Context		Delay												
Context		Structural strength												
Context		Barriers												
Context		Security containers												
Context		Locks/cylinders												
Context		Response												
Context		Professional practice												
Context		Engineering design process												
Context		Analysis & evaluation												

Similar **Dissimilar**

Context		Situational crime prevention												
When compared to				**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	
Security planning & design		Environmental conditions												
Security planning & design		CPTED												
Security planning & design		Defence in depth												
Security planning & design		Movement control												
Security planning & design		Surveillance												
Security planning & design		Detection												
Security planning & design		Technology												
Security planning & design		Lighting												
Security planning & design		Sensors												
Security planning & design		CCTV												
Security planning & design		Delay												
Security planning & design		Structural strength												
Security planning & design		Barriers												

Appendix F

PHASE 4 FOCUS GROUP SEMI-STRUCTURED INTERVIEW QUESTIONNAIRE

Curtin University
School of Science and Mathematics Education Centre

Focus Group Interview Invitation: Participant Information Letter

This research study is being undertaken as part of the requirements for the award of Doctor of Philosophy (PhD) of Science and Mathematics Education at Curtin University in Western Australia.

Aim: To undertaking a cultural domain analysis to identify a formal knowledge system (body of knowledge) for the domain of physical Security.

Guidelines: Your participation in this research phase will require you to attend a one hour focus group interview. If you agree to participate in this study every effort will be made to find a convenient date, time and location which suit all participants agreeing to participate.

Risks and Discomforts: There are no foreseeable risks or discomforts associated with your participation in this study. However, you are requested to provide an hour of your time and be willing to have the interview recorded to enhance analysis and for reliability validity purposes.

Confidentiality: Information obtained from this study which could identify you will be kept private to the extent allowed by law. The information you provide will be kept separate from your personal details and only I and research supervisors will have access to this. The interview transcript will not have your name or any other identifying information on it and in adherence with university policy, the interview tapes and transcribed information will be kept in a locked cabinet for at least five years, before a decision is made as to whether it should be destroyed.

Consent to Participate: Your involvement in this study is entirely voluntary and you have the right to withdraw at any stage without affecting your rights or my responsibilities. Once you have signed the consent form, it will be acknowledged that you have agreed to participate and allow me to use your data in this research.

Further Information
This study has been approved by the Curtin University Human Research Ethics Committee (Approval Number HR xx/2012). The Committee is comprised of members of the public, academics, lawyers, doctors and pastoral carers. If needed, verification of approval can be obtained either by writing to the Curtin University Human Research Ethics Committee, c/- Office of Research and Development, Curtin University, GPO Box U1987, Perth, 6845 or by telephoning 9266 2784 or by emailing hrec@curtin.edu.au
If you would like further information about the study, please contact myself Michael Coole; 08 63045123, or email: m.coole@ecu.edu.au or,
Professor David Treagust on 08 92667924, or email: D.Treagust@curtin.edu.au or, Dr Dave Brooks; 08 63042827, or email: d.brooks@ecu.edu.au

Study Consent Form

Thank you for choosing to participate in this research study, please read the terms of informed consent below.

- I understand the purpose and procedure of the study.
- I have been provided with the participation information sheet.
- I understand that the procedure itself may not benefit me.
- I understand that my involvement is voluntary and I can withdraw at any time without a problem.
- I understand that no personal identifying information such as name and address will be used in any published materials.
- Í understand that all information will be securely stored for at least 5 years before a decision is made as to whether it should be destroyed.
- I have been given the opportunity to ask questions about this research.

Your signature below indicates that you consent to participate in this study.

I_____ agree to participate in this research study. In line with the requirements of informed consent, I provide my consent.

Signature_____ Date_____/____/____.

This document was witnessed by Michael Coole_____
Date____/___/____.

Focus Group Interview Research Questionnaire

The jurisdictional focus for Physical Security is directed towards the diagnosis, inference and treatment of security or loss coupled risk concerns associated with people, information and property manifested through unlawful access plus crime enablers in the protection of assets. Such treatment results in a security function as an organised complex of specialised technological, physical and procedural elements integrated into a protective barrier system.

Phases One, Two and Three of the study provided knowledge requisites (Tables 1, 2 & 3) and propositional maps (Figures 1 & 2) for understanding the knowledge domain of physical security. These maps have drawn out a vast number of knowledge concepts, principles and theories as core and subordinate concepts from the domain of physical security. One map (Figure 1) is derived from a qualitative analysis showing local connections, and the second a broader map (Figure 2) established through perceived ratings of similarity and dissimilarity showing macro structure organised according to clusters of knowledge relating to the professional dimensions of practice.

Curriculum development entails the identification, selection and organisation of a set of intended learning outcomes. This should be based on educational goals in terms of what is to be learned. The goals indicate why it is to be learned (Posner & Rudnitsky, 1982, p. 8)

Phase 4 Research Question: What are the learning objectives and knowledge requisites for physical security professionals?

Key points: The reviewed literature highlighted a number of salient points for professional education:

h) The need to consider the broader goals;
i) Units should be planned in context with other units-relationships;
j) Sequence-planned, where units both precede and follow other learning units;
k) Should teach the science or knowledge that the domain is built;
l) Learning of principles and attitudes;
m) General graduate attributes;
n) Content- scope- organisation-sequence.

Accordant with these key points, Eraut (1994, p. 119) highlights three key questions for every profession:

E. What is the professional knowledge base?
F. What is best learned in higher education?
G. What is best learned in professional practice, and what is best learned through an integrated course involving both contexts?
H. What has to be learned before qualification, and what is best postponed until after qualification?

Interview Questions:

1) In terms of articulating a formal knowledge system, based on these maps, what do you see as the foundation knowledge unit requirements to be learned by physical security professionals before qualification?

2) It is argued that higher education students should learn or know the science or knowledge of which their future domain is built. Based on this view, what is the depth of scope or focus for security higher education knowledge?

3) Do you believe these maps capture the knowledge concepts required for a physical security professional, if not what do you consider is missing?

4) What should be learned after qualification, in professional practice?

5) Based on learning principles how should these knowledge units be organised?

6) What are the strengths and perhaps the weaknesses of these maps in terms of establishing a physical security professional's knowledge system?

7) Based on what has been discussed so far and the knowledge heuristics, what are the higher education learning objectives for future physical security professionals?

Appendix G

PILOT STUDY PHASE 1 MERGED SYNONYMOUS TERMS

Book	**Category**	**Merged terms**
Book 1	Entry control/Access control	Entry control, access control
	Closed circuit television - CCTV	CCTV, closed circuit television
	Analysis and evaluation	Analysis, analysis and evaluation
	Facility procedures	Procedures, facility procedures
	Alarm assessment	Alarm assessment, video alarm assessment
	Target identification	Targets, target identification
	Threat	Threat, threat definition
Book 2	Closed circuit television - CCTV	CCTV, closed circuit television
	Fire	Fire, fire protection
Book 3	Analysis and evaluation	Analysis, analysis and evaluation, EASI model and analysis and evaluation methodological approach
	Closed circuit television - CCTV	CCTV, closed circuit television
	Facility characterization	Facility, facility characterization
	Use of force	Neutralization. Use of force, arrest
	Law	Legal issues, law
	Traffic control	Traffic, traffic controls
	Loss prevention	Theft controls, loss prevention
	Detection systems	Detection, alarm systems
	Safes and vaults	Safes, safes and vaults

Appendix H

STUDY PHASE 1 MERGED SYNONYMOUS TERMS

Book	**Category**	**Merged terms**
1	alarm	alarm, alarms
	assessment	assess, assessment
	assets	asset, assets
	attack	attack, attacks
	CCTV	camera, cameras, video, CCTV
	communication	communication, communications
	control	control, controls, controlled
	design	designed, design, designing
	detection	detects, detection, detecting, detected, detect
	devices	device, devices
	door	door, doors
	entry	enter, entry
	facility	facility, facilities
	fences	fence, fences
	fields	field, fields
	guard	guard, guards
	level	level, levels
	lighting	light, lights, lighting
	measurement	measure, measures, measured
	people	people, persons, person, personnel
	sensor	sensor, sensors
	system	systems, system
	technology	technology, technologies
	threat	threat, threats
	zones	zone, zones
	response	response, respond
	barriers	barrier, barriers
2	system	systems, system
	CCTV	camera, cameras, video, CCTV
	alarms	alarm, alarms
	threat	threat, threats
	doors	door, doors
	sensors	sensor, sensors
	locks	lock, locks
	facility	site, area, facility

3	alarms	alarm, alarms, alarm systems
	assessment	assess, assessment
	CCTV	camera, cameras, video, CCTV
	control	control, controls
	design	designed, design
	devices	device, devices
	doors	door, doors
	fence	fence, fences, fencing
	guards	guard, guards
	level	level, levels
	lighting	light, lights, lighting, lighted
	sensor	sensor, sensors
	system	systems, system
	threat	threat, threats
	attack	attacks, attack
	barriers	barrier, barriers
	bolts	bolt, bolts
	building	building, buildings
	costs	cost, costs
	crime	crime, crimes
	criminals	criminal, criminals
	cylinder	cylinder, cylinders
	electrical	electrical, electronics, electrics
	fire	fire, fires
	glass	glass, glazing
	images	image, images
	interior	interior, internal
	lens	lens, lenses
	locks	lock, locks
	network	network, networks
	pins	pin, pins
	protection	protect, protection, protecting, protected
	risk	risk, risks
	safes	safe, safes
	signal	signals, signal
	standards	standard, standards
	tumbler	tumbler, tumblers
	windows	window, windows
	combinations	combination, combinations

4	alarms	alarm, alarms
	assessment	assess, assessment, assessments
	CCTV	camera, camera, CCTV
	control	control, controlled
	design	designed, design, designer
	detection	detection, detectors, detector, detect
	devices	device, devices
	doors	door, doors
	entry	enter, entry, entrance, entrances
	system	systems, system
	sensors	sensor, sensors
	technology	technology, technologies
	threat	threat, threats
	lighting	light, lights, lighting
	fire	fire, fires
	images	image, images, imaging
	locks	lock, locks, locking, locked
	risk	risk, risks
	biometric	biometric, biometrics
	business	business, businesses
	costs	cost, costs
	guards	officer, officers, guard, guards
	identify	identify, identification, identified, identity
	intrusion	intrusion, intruder, intruders
	keys	key, keys
	leadership	lead, leader, leadership, leads
	level	level, levels
	organization	Organization, organizational and company
	planning	plan, planning
	protection	protect, protection, protected
	visitor	visit, visitor, visitors
	building	buildings, building
5	intrusion	intrusion, intruder, intrusions, intruders
	alarms	alarm, alarms
	assessment	assess, assessment, assessed
	assets	asset, assets
	attack	attacks, attack

	barriers	barrier, barriers
	CCTV	camera, cameras, CCTV
	communication	communication, communications
	design	designed, design
	detection	detects, detection, detecting, detected, detect
	doors	door, doors
	facility	facility, facilities, facil
	fences	fence, fences
	lighting	light, lights, lighting
	protection	protect, protection, protecting, protected
	sensors	sensor, sensors, sensing
	adversary	adversary, adversaries, adver
	analysis	analysis, analyses, analyst
	components	component, components
	delay	delay, delayed
	evaluation	evaluate, evaluation, evaluating, evaluated
	maintenance	maintain, maintained, maintenance
	material	material, materials
	reports	report, reports, reported
	response	response, responses, respond, responds
	testing	test, testing, tested, tests
	vulnerability	vulnerability, vulnerable, vulnerabilities
	control	control, controlled, controller, controls
	system	system, systems
6	assessment	assess, assessment
	design	designed, design
	doors	door, doors
	electrical	electrical, electronics, electric
	evaluation	evaluate, evaluation, evaluating
	identify	identify, identification, identified, identity
	level	level, levels
	lighting	light, lights, lighting
	planning	plan, planning, plans
	protection	protect, protection, protected
	report	report, reports, reporting
	response	response, responses, respond
	system	systems, system
	testing	test, testing, tests
	vulnerability	vulnerability, vulnerable, vulnerabilities

	cable	cable, cables
	cards	cards, card
	document	document, documentation, documented
	drawings	drawing, drawings
	installation	install, installed, installation, installations
	meeting	meeting, meetings
	monitoring	monitor, monitors, monitoring
	recommendation	recommend, recommended, recommendation, recommendations
	requirements	requires, requirements, requirement
	review	review, reviews
	acceptance	acceptance, accept, acceptable
	CCTV	camera, cameras, CCTV
	control	control, controlled, controls
	devices	device, devices
7	alarms	alarm, alarms
	biometric	biometric, biometrics
	cables	cable, cables, cabling, coax
	CCTV	camera, cameras, video, CCTV
	communication	communication, communications, communicate
	costs	cost, costs
	design	designed, design, designing
	detectors	Detector, detectors
	doors	door, doors
	electrical	electrical, electronics, electric, electronic, electronically
	field	field, fields
	level	level, levels
	lighting	light, lighting
	monitoring	monitor, monitoring
	protection	protect, protection, protected
	sensor	sensor, sensors
	standards	standard, standards, standardized
	system	systems, system
	technology	technology, technologies
	testing	test, testing, tested
	applications	application, applications
	automation	automation, automatic, automatically
	badges	badge, badges
	devices	device, devices

	employees	employees, employee
	functions	functions, function
	installation	installation, install, installed, installing
	location	locations, location, located
	panel	panel, panels
	project	project, projects
8	alarms	alarm, alarms
	barriers	barrier, barriers
	cards	cards, card
	CCTV	camera, cameras, video, CCTV
	communication	communication, communications, communicating
	control	control, controls, controlled, controllers
	design	designed, design, designing
	detection	detection, Detect
	devices	device, devices
	doors	door, doors
	drawings	drawing, drawings
	electrical	electrical, electronics, electric, electronic
	guards	guard, guards
	locks	lock, locks
	monitoring	monitor, monitors, monitoring, monitored
	networks	network, networks
	project	project, projects
	system	systems, system
	technology	technology, technologies
	interface	interface, interfaced, interfaces, interfacing
	transmission	transmission, transmit
	contractor	contractor, contractors
	detectors	detector, detectors
9	analysis	analysis, analyses
	applications	application, applications
	attack	attacks, attack, attacking
	CCTV	camera, camera, video, CCYV
	communication	communication, communications, communicate
	detection	detection, Detect
	devices	device, devices
	leadership	leader, leadership, leading

	level	level, levels
	monitoring	monitor, monitoring, monitored
	networks	network, networks, networking
	protection	protect, protection, protecting, protected
	sensors	sensor, sensors
	standards	standard, standards
	system	systems, system
	technology	technology, technologies
	policy	policy, policies
	server	servers, server
	integration	integrate, integrated, integrating, integrator
	model	model, models
	logical	logic, logical
	environment	environment, environments, environmental
	vendors	vendor, vendors
	computers	computer, computers, computing
	response	response, respond
10	building	building, buildings
	costs	cost, costs
	level	level, levels
	material	material, materials
	protection	protect, protection, protective
	risk	risk, risks
	standards	standard, standards
	system	systems, system
	testing	test, testing
	incident	incident, incidents
	training	train, training
11	alarms	alarm, alarms
	assets	asset, assets
	communication	communication, communications, communicate
	costs	cost, costs
	crime	crime, crimes, criminals
	facility	facility, facilities
	incident	incident, incidents
	level	level, levels
	organization	Organization, organizations

	planning	plan, planning
	protection	protect, protection, protecting, protected, protective
	report	report, reports
	response	response, respond, responding
	risk	risk, risks
	system	systems, system
	threat	threat, threats
	training	train, training, trained
	law	legal, law
	prevention	prevent, prevention
	terrorism	terrorism, terrorist, terrorists
	weapons	weapon, weapons
	people	people, personnel, staff
	hazards	hazard, hazards
	detection	detection, detect
12	alarms	alarm, alarms
	attack	attacks, attack
	building	building, buildings
	cards	cards, card
	control	control, controls, controlled
	costs	cost, costs
	crime	crime, crimes, criminal
	design	designed, design
	devices	device, devices
	doors	door, doors
	internal	interior, internal
	keys	key, keys
	law	legal, law, laws
	lighting	light, lighting
	locks	lock, locks, locking, locked
	people	people, persons, personnel, individuals, employees
	policy	policy, policies
	prevention	prevent, prevention
	protection	protect, protection, protecting, protected, protective
	reports	report, reports, reported, reporting
	risk	risk, risks
	standards	standard, standards
	terrorism	terrorism, terrorist, terrorists, terror
	loss	loss, losses

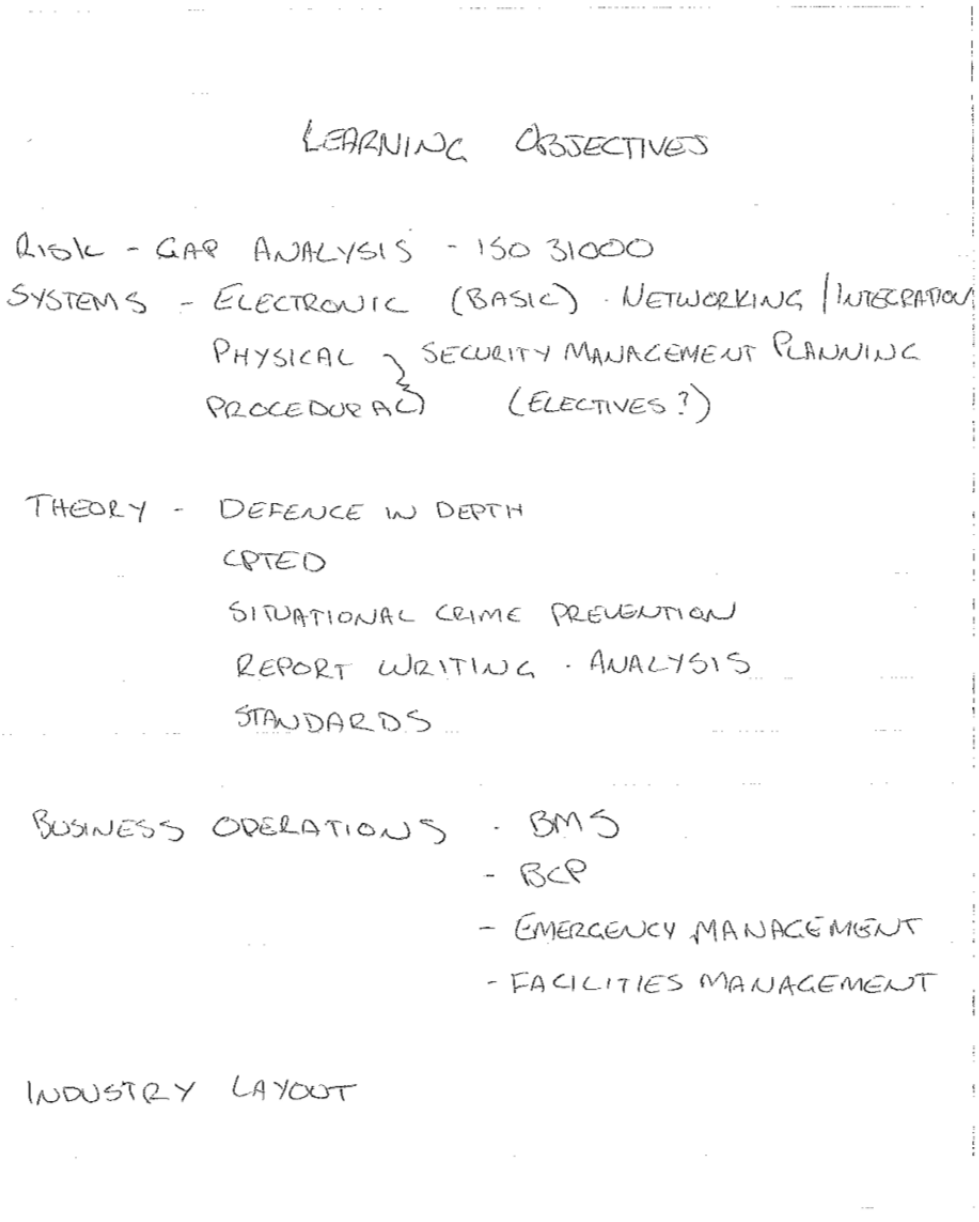
	theft	theft, thefts
	facility	facility, facilities
	planning	plan, planning
	response	response, respond, responses
	threat	threats, threat
	level	level, levels
	surveys	survey, surveys
13	alarms	alarm, alarms
	application	application, applications
	assets	asset, assets
	attack	attacks, attack, attacker
	barriers	barrier, barriers
	biometric	biometric, biometrics
	control	control, controls, controlled
	costs	cost, costs
	environment	environment, environments, environmental, environ
	evaluation	evaluate, evaluation, evaluated
	Organization	Organization, organizational, Organizations
	people	people, person
	planning	plan, planning, plans
	response	response, respond
	risk	risk, risks
	standards	standard, standards
	system	systems, system
	technology	technology, technologies, technological, technical
	testing	test, testing, tested
	threat	threat, threats
	assessment	assess, assessed, assessing, assessment, assessments
	concepts	concepts, concept
	context	context, contexts
	critical	critical, criticality
	decision	decision, decisions
	principles	principle, principles
	process	processing, process, processes
	resources	resource, resources
	strategy	strategy, strategies
	detection	detection, detected, detecting
	protection	protection, protecting, protected

14	alarms	alarm, alarms
	assets	asset, assets
	building	building, buildings
	CCTV	camera, camera, CCTV
	costs	cost, costs
	crime	crime, crimes
	design	design, designing, designer
	environment	environment, environments, environmental
	facility	facility, facilities
	fences	fence, fences, fencing
	lighting	light, lights, lighting
	standards	standard, standards
	system	systems, system
	terrorism	terrorism, terrorist
	vulnerability	vulnerability, vulnerabilities
	zones	zone, zones, zoning
	access	access, entry
	codes	code, codes
	employees	employee, employees
	people	people, public
15	assets	asset, assets
	bolts	bolt, bolts
	building	building, buildings
	cards	cards, card
	CCTV	camera, cameras, video, CCTV
	crime	crime, crimes, criminal, criminals
	design	designed, design, designing
	detection	detection, detect, detector
	devices	device, devices
	doors	door, doors
	facility	facility, facilities
	fences	fence, fences
	guard	guard, guards
	interior	interior, internal
	keys	key, keys
	level	level, levels
	lighting	light, lights, lighting
	locks	lock, locks,

	people	people, personnel, staff
	planning	plan, planning
	response	response, respond
	standards	standard, standards
	procedures	procedure, procedures, process, processes
	vehicles	vehicle, vehicles
	alarms	alarm, alarms
	attack	attack, attacks

Appendix I

PHASE FOUR PARTICIPANT'S LEARNING OBJECTIVES



LEARNING OBJECTIVES

RISK - GAP ANALYSIS - ISO 31000
SYSTEMS - ELECTRONIC (BASIC) · NETWORKING / INTEGRATION
PHYSICAL } SECURITY MANAGEMENT PLANNING
PROCEDURAL (ELECTIVES?)

THEORY - DEFENCE IN DEPTH
CPTED
SITUATIONAL CRIME PREVENTION
REPORT WRITING · ANALYSIS
STANDARDS

BUSINESS OPERATIONS · BMS
- BCP
- EMERGENCY MANAGEMENT
- FACILITIES MANAGEMENT

INDUSTRY LAYOUT

(4)

- Supply chain Security.
- Convergence Between IT & OT's
- Mapping of Employment Pathways.

(2)

LEARNING OBJECTIVES:

- SECURITY CONCEPTS & THEORIES.
  - DiD, CPTED, SCP, Detect, Delay, Respond, Recover etc..
- Security Planning & Design.
  - Design objectives.
  - Architectural drawings.
  - Construction framework (i.e what happens)

(3)

- locking system < electronic / physical
- Standards / legislation.
- Framework of safety.
  - CIP
  - Linkages with HSE & others.
  - Defence
  - Government.
- Understanding of the Value Add.
- Asset protection Continuum.
  - Identify
  - Assess
  - Plan
  - Respond
  - Recover
  - Learn.

①

- Language - Big barrier - Many people have many different viewpoints & Understanding of many aspects of Security.

- What is the basic knowledge required from a graduate?

- Systems Theory → Analysis & Design
- Security Concepts & Theories.
- Electronic Security → CCTV, Detection Sensors, Electronics 101
- Security Risk Management.
- Protection.
- PM. → Contracts, Mgt, Planning, Organising.
- Design Documentation (Security Planning & Design)
- History of Security - Why do we do it?
- Locking Systems → electronic, physical.
- Standards / Legislation.

PATHWAYS.

- Systems Theory: an indepth understanding of the theory, which would lead the student to develop their ability to contextualise, and then analyse the threat/risk, treatments etc.

- Ability to read + interpret, design docs - including drawings as well as specifications.

- Understanding the function within the context of broader disciplines.

- To inform industry proponents on what the degree delivers, and why the professionals are related to delivering the goals and objectives of industry.

→ 10,000 foot view.
→ know enough to know what you don't know.
→ know where to find more information.

* know how light, sound, movement may be used to detect & deter
* know about currently available technologies and their limitations - broad & shallow.
* know how to use & apply the technologies tools & how they assist management.

LEARNING OBJECTIVES.

(1) RESEARCH ABILITY TO KEEP UP TO DATE WITH NEW & EMERGING TRENDS IN SECURITY.

(2) KNOWLEDGE & APPLICATION OF RISK MGT FRAMEWORK.

(3) ~~CONVERGENCE~~ CONVERGANCE OF TECHNOLOGY & HUMAN FACTORS IN SECURITY.

(4) BUSINESS COMMUNICATION SKILLS

(5) PROJECT MANAGEMENT SKILLS.

GARRETT THOMAS

→ Design Management

→ linkages to other business functions

→ How to add value

→ Security Theory / concepts

→ linkages to other security functions

→ Risk

☆ Does not

→ show percentage of relevance

→ link or order to how could be taught

Brian

Access control & Sensors as one unit

how - in each unit as it fits ie
Acts, Regs.. Standards.

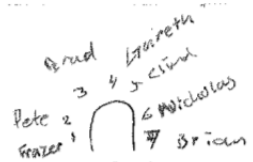
Risk,
Security Planning & Design
Building management Systems
Security Surveys / Audit & Reviews

People, data & info Property infrastructure.
and how it relates to Security

CPTED

Appendix J

PHASE FOUR'S INDEPENDANT NOTE TAKER'S NOTES



1

4 = understanding of risk, know security concepts & theories (DiD etc)

1 = needs to have an understanding of the technical side = how the tech works, what it does etc in order to

3 = shallow broad knowledge, top down approach, risk understanding. Agrees with 1's answer, however thinks its more important to know what is possible & what is not and then seek out & tech expert for the rest. Tech experts are different & usually narrow in their skills

4 = Two personality types - some people are tech inclined, some report writers = very difficult to find someone with both skills and we need the two personalities to bounce off each other

2 = Confidence, high level overview as part of degree Seperate what they are learning = a security professional is not a cyber or it person. Maybe name it a physical security professional

1 = There needs to be a broad / baseline undergrad degree & then you are to specialize in an area post graduate - like law degrees etc.

6 = Risk! Its the most essential thing. Deep knowledge of risk = be able to write up a risk assessment report & risk treatment

2 = Balance between threat & risk treatment

6 = You also need core knowledge → to be able to understand & be able to identify why / who not something works or will not work for a specific purpose

1 = Qualitative Risk Assessments → need the foundational principles of that. Personalities are important - consultants

$\prod_{i=1}^{n}$

= Mgmt of the design. The phases you have to go through to develop the final products. How to communicate and who needs to know what.

= Agrees with 4 but thinks it gets developed after the degree

= Contract Mgmt

4 = English & Maths is the basics (Foundation)
writing technical side.
So they can communicate with both technical & the abstract people.

= Understanding of threat and try and define what it is from a physical security perspective - its so subjective

= Prioritise Figure 1 = hierarchy
systems theory needs to be high up
Qualitative/Quantitative Risk

= Systems theory will help with understanding all the rest → then break it down

2 = Report writing - not essays

3 = Very high and basic understanding of risk
Common sence
Critical & logic reasoning

1 = Communication skills
Project Management skills

4 = someone who is not afraid of saying = i dont know this

2 = Attributes will be different dependent on what consultancy firm/job they will be at

1 = The concepts of security (theories & principles)
↳ most of the stuff in the yellow of Figure 1

6 = ISO 31000 → Follow the structure of this FW
Context → Risk → Treatments → Risk Acceptence →

.= Project management, systems theory, infrastructure protection, → Bring all the concepts together
Electronic security
Theories etc

1= what it isn't = law & adversary criminology
2= ↳ maybe rather the knowledge of standards and have a general understanding of regulations would be better
↳ I need to know what makes up a threat but not a deeper understanding
3= from a knowledge perspective it nn to be there (adversary criminology)
2= But it could be encompased in threat knowledge
4= I dont need to know why someone commits a crime or how society can treat that as a consultant
- Ergonomics is also not really important → its something i need to know exists but not in any depth → this can come later
5= You also need to know what does come later
1= Tech understanding
Physical security
Risk
Project Mgmt
4= The person who understands how security can add value to an organisation → the linkages between everything
↳ identify where the value adding priciples are
6= Safety = unintentional acts
Security = intentional acts
7= licensing
2= Analysis is important
↳ The ability to be able to find out what you need to

4 = Analysis is core (agrees with 2)
Its a process = getting it to the nuts & bolts of things
2 = Confidence in knowing how to analyse information
7 = Hands on work / Placement is important
2 = Figure 1 is confusing (novices)
A hirical Flowchart would be better
1 = Engineering has developed good Flowcharts related to what you need to go into dependency on where/what area you want to go into
2 = Safety is prescribed in legislation, security is not
1 = ASIS international is the only basis so far
but its not really a good measure.
4 = where it sits/ Fits
→ linkages
↳ basic principles of where it adds value & how to achieve this
1) Personality types are so important
↳ but that is seperate to a syllabus
4 - understanding of what we actually do
↳ a base at the beginning and then introduce them to the different areas they can choose from
3 = a broad understanding of everything on Figure 1
2 = to understand & articulate what is being discussed
ie broader understanding of everything
7 = Defeate
Operate
how quickly defeat
key control
cylinders
typologies of locks, major components of locks, how to defeat it & how it works
→ Basic function of how a lock works
→ Cylinder

3 = - Basic understanding of the laws of physics
- How to apply them in detecting & threat

6 = How things connect (integration)

3 = Electronic security is a tool (ends to a means)

6 = less focus on technology & more the understanding what you do with it

1 = - Relevant Standards & Legislation
- How physical → electronic → risk fits/links together
- Overarching Principals
- understanding at a higher level how risk fits in to every day life

4 = - understanding of the process & ideally what it should look like so that they can identify the gaps when meeting client so that they can then add value

Appendix K

PHASE TWO PARTICIPANT INTERVIEW TRANSCRIPT

Michael Coole _ Braden

MC: The first table is this one Braden and it is a list of knowledge categories on their own, the argument is that any cultural domain, when you look at physical security, it is actually a cultural domain, we see it as a profession but it actually comes from a cultural domain and that is based on a single semantic relationship with a cover term which for us is security. When I did the count check analysis it worked out well for me because security came up as the top thing. What that means to us as educators is that the first thing we have to teach is the concept of security, you have to know what you are trying to attain. In terms of say system, a lot of the feedback is that that is not so much as functional systems but systems theory, how we integrate components together to achieve our objective according to that plan, there is no point putting something into the system that is going to be more disruptive than good. Is there anything you don't understand? They are the top 49 categories from all the different text. One of the things with this I didn't have control of the raw table that is what comes out of the literature extraction. The theory behind that is the experts in the domain are the ones who write the text books so what occurs more frequently in the printed text it captures that domain space. The other one I've got is table 1, this is what some of the knowledge concept categories that some of the other experts said this is what you are missing. For instance, one of the participants said door furniture, hinges locks all that becomes under door furniture for them from a project management perspective. Things like understanding structural strength, one guy said the concept of surveillance supersedes CCTV and CPTED so you need to understand what the surveillance objective is and then how do we achieve that. Are there any that you disagree with in here?

BRADEN: Nothing I disagree with , a few of them I would think you would categorise in similar things, for example field review lenses to me is CCTV, straight away I would be thinking that is under CCTV, they are probably the things, like devices again you've got senses and devices.

MC: Yes, one guy said devices should be removed.

BRADEN: I think categorising these into smaller categories is something that stands out.

MC: One of the things I will do is go through concept reduction, say this is super ordinate to this and this is subordinate, and in fact this table that is what we have tried to do, the order of this is how they appear in the extracted text so where CPTED comes up is where it came up as an numerical count analysis, across all the text and that is one of the things, basically this provides a matrix of knowledge areas, things like access control, so we know a key area of physical security is controlling access and what is interesting is the concept of control is one of the things that comes up often, anything to do with physical security that's what we are trying to achieve.

BRADEN: Nothing I don't disagree with, more and more I think communications and infrastructure will come up more, I think that is what we are seeing come

through in the last 5 years or so.

MC: When you are talking about communication are you talking about the ability to communicate with clients both written and that or are you talking about communication technology?

BRADEN: Communication technologies, so infrastructure, networks so sort of the merging between your traditional systems, electronic access control, CCTV and how they communicate so communication technology, that is definitely something that is becoming more and more important especially we are now sharing communication technologies with other technologies not only security technologies so that is becoming more and more important as well.

MC: One of the guys said network fundamental is vitally important, would you agree with that?

BRADEN: Definitely. That is the communicat8ion method of how we are actually emerging and integrating all these technologies.

MC: That seems to be coming up and I mean here it has networks and what does that really mean, networks keeps coming up and the other thing, one of the things that they've done at the ECU course is put in an option for a cyber-security stream within that degree as a major, and that is becoming quite popular.

BRADEN: I do see the two quite separate, the network fundamentals is essential for a security consultant and for what we do because we need to understand how do networks work and what sort of infrastructure do we need to put in to make sure our systems can communicate, the fundamentals is what we need to know. Do we need to know about cyber security when we are putting those things together – probably not; do we need to understand the fundamentals – yeah.

MC: I did a thing on CCTV Wi-Fi vulnerabilities and it was quite easy to hack a lot of the Wi-Fi systems.

BRADEN: I know a few clients here that basically the hard wire they protect but as soon as they put in Wi-Fi hot spots all of a sudden there is a back door into getting footage out of the cameras on the site. They are completely oblivious until a contractor says "that is how we configure our cameras, we just use your Wi-Fi".

MC: Do you think there is anything missing then, apart from networks, is there anything that you felt you would have been better to be abreast of? One of the guys last week said project management.

BRADEN: I would agree with that because we, generally a client will come to us and they want to roll out a security project and then we then become almost the project manager for that project. On behalf of the client we go out to tender and select contractors, we do an evaluation on behalf of the client and then we will recommend what contractor should do the work and then when it is being implemented we then manage them and make sure they have a program of works that meets the clients expectations and then follow up and make sure it is installed as per specifications.

MC: So then that generally includes contract management as well?

BRADEN: Yes, contract management, being superintendent.

MC: A lot of these things, some of them were taught in the old ECU degree and some of them have been dropped off and once again this is purely for looking at a general education framework so it doesn't matter if a US

university or a Sydney university wants to teach it, it is what are those broader knowledge categories that combine to produce someone. Also the focus is someone who goes out, one of the things that is becoming clearer is – you need to go out as a graduate. You are not going out just because you've done a degree as this person up here, a lot of people think if I do a degree, whereas if you look at medicine, accounting, all these other professions – you go into a graduate position, even law you graduate from law and you go through that graduate process, in the intelligence domain they call it the journey man where it takes you two years to turn you into a competent person.

BRADEN: Definitely. SKM Jacobs they have done that, so when we are employed we go through a four year graduate program with all the other engineers, and that is all about having that graduate title to say you have done your degree but you are a graduate for four years until the senior people in the business believe that you are up to the standard of being a security consultant.

MC: That is good to know actually. What this table has done here and you can see the idea is that this table has organised the concepts hierarchically and then this figure just flows off. So the argument is all this figure is a heuristic that connects the hierarchical table so that is the raw categories just organised based on some of those principles. I guess with that do you think any of them need to be relocated, do you think that we have captured, some of it not all of it is going to be linear, although we are trying to capture that relationship.

BRADEN: CPTED is an interesting one, being under the – if you see that as a technology and you've got all the technologies down one side, CPTED being associated to a technology I think is potentially in the wrong location. I wouldn't say it's a technology, definitely associated to surveillance but not necessarily technology.

MC: so where would you put it?

BRADEN: I guess you've got defence in depth and situation crime here with emergency so potentially under facility procedures, but associated to situational crime prevention. I see those two things related.

MC: That's a good point. This is one of the hardest things to try and get an understanding of how that knowledge is organised, how the hierarchical concepts are related.

BRADEN: I think security surveys and risk are associated to some extent, usually if you are doing a survey it is part of the risk processes that you are undertaking. I see you have risk up the top that sort of includes everything so that is probably right. It all makes sense.

MC: The idea of that is to produce a heuristic, just a rule of thumb. It's just about having a diagram to represent how knowledge is related or fits together like that, do you see any problems with developing that from that table, looking at it that way should we probably include it or should it be changed about?

BRADEN: I think graphically it makes sense. The infrastructure one sort of jumps out a little bit that you are including everything under infrastructure, I guess the definition of infrastructure is probably the thing that is hardest to define, when I see infrastructure I think of network infrastructure probably more than anything else, but understand the terminologies would include a lot more than that.

Sharne & Michael Coole

SHARNE: So far in principle I agree with everything that you have said, I'm not sure that I totally see this particular model or table here being of much value and probably end up asking more question than answers, because some of it 100% relevant and the rest of it to me stands out in isolation. The principle would be rather than doing that I would be looking at categorising those things. I suppose a bit about me, I'm a graduate from the ECU course, I think I was the second graduating year so quite early in the piece, since leaving I've been in consulting for 15 years now, so quite limited in terms of industry expertise, in only having exposure to consulting engineering and the practices we do rather than some others, like my brother qualified in the year after me at the same course at the same time, he spent a year or two out at security operations as a security manager for Woodside Building, so we have similar backgrounds. I don't know how the course has moved on or evolved since Cliff Smith originally put it together and I'm not intending to make comparisons except to say the way we were taught seems more logical, all the same principles there, it's been 15 years plus since I've touched basis with the course and I don't know how they still do it, but at the time it seemed to me to be quite logical and I think back to how I learnt, seems a little bit more logical than what I'm seeing here, which is a random series of ideas. Just on that, the way they roughly broke it up then and I think it is pretty good background for anybody who are looking to come into the industry, it was based on a series of categories so you had physical security 1, 2, under the physical security 1 it took care of all the absolute fundamentals – locks, barriers, keys, all of the principles, physical security 2 then started to look into some of the slightly more complex elements of physical security so you've gone beyond safes, vaults, locks, keys and started to look how you put those physical barriers together to come up with a physical solution. Then I think there was computer security, there was security risk management – so a whole bunch of quite logical categories which all this stuff fits into. It just seems a little bit more logical, if I look back now after the experience, I've also employed a lot of graduates and worked with a lot of graduates both coming from the course and coming from industry, I think one of the good things about the background I got out of the course was initially it was very broad, the negative side to that is that there wasn't very much focus post. So they had really good broad background knowledge in terms of the subjects they looked at, then in terms of security management we had security risk management 1 and 2 and it covered all of it broadly, other than that you got a degree in security and you had to go and do a minor of business management. So I think if there was a more tailored end to it.

MC: And that is what this is about, trying to get a focus for people.

SHARNE: If I look at that now I got a minor in business management. I can see criminology being relevant if you are interested in that field. A lot of people I came across at the time either did the criminology course or went and did the minor at criminology at ECU. You mentioned it early when you were talking about statistical analysis, that is almost a totally separate issue to

what physical security professionals do, there is plenty of people out there that do risk analysis on theoretical statistical analysis, wouldn't know the first thing about how to protect something, I would almost say that in itself, the whole criminology side, is a totally different stream in itself. But so if that is what you are looking at then absolutely I think it would make sense to have a degree as a psychical security professional, and then even in what we do now, out of some of these categories that you are talking about, as I was say within our career and within our team we have got people that come from an engineering background you've got people like myself that come from quite a general background so I'm learning the engineering on the job. When you flip that the engineers don't understand the fundamentals like crime prevention, environmental design, defence in depth all those principles, they have learnt that on the job. I think the ability to look at the market sector that you are considering going into it kind of makes sense that you should be able to specialise in risk or specialise in design and engineering or specialise in computer security and ICT, cyber security.

MC: That is the way it is going, a lot of them are doing different minor and major sets to support that very notion. What I'm trying to say is in the physical security text so what I've done is I've going into the security text, 15 of them, and I've extracted from each text the top 49 security areas, so risk and threat things like that and then I combine it as a summation and that is what this is pulled out. Something that has come forward, when I did the initial category stuff so you get this category here, some of the experts I interviewed earlier said you haven't got things like door furniture which is super-ordinate to locks and hinges so architects talk in terms of door furniture; defence in depth is a thing that doesn't come up very often in terms of its saliency, things like surveillance is an overarching concept for CCTV, structural strengths – how do we know what the engineer is telling us in terms of that so what I'm looking at today in the first part and things like that. So what I'm looking at today is to ask are there any of these knowledge areas that you don't think are relevant to physical security or are there any that are missing. One of the guys said earlier, I wish I had of learnt to read architects plans and I never did.

SHARNE: I think that is a valid point as an example, again it becomes a little bit confusing around what we are trying to achieve here, are we trying to produce graduates that can come out of the course and go into a design related type field such as consulting or is that too focused.

MC: No, what I'm looking at is a security person, could be Diploma in Physical Security or a graduate from a university course, not just Edith Cowan and I'm saying someone who is a Protective Security Adviser, so in Federal Government they have PSAs, Dept of Defence and ASIO has PSAs, in the consulting world we are called consultants, I'm looking not so much Security management but how people look at and diagnose a security problem and I suppose design a security system to treat that problem but I'm looking at a graduate. I'm not saying when you graduate you should be the equivalent of someone with 12 years' experience because it's not practical. If you look at someone in accounting, graduates go to a graduate position, nurses go into a graduate position, doctors are the same they become interns. A friend of mine who graduated from law was carrying books for a

year, all these other professional areas recognise that someone coming out of university is a graduate, if you look at psychology you graduate from university, you have to do your registration and supervision under that. What I'm saying is - what is the knowledge we want someone to graduate with that then we can professionally develop them over time. Because one of the things that security has done poorly in the past is we believe that we are training people that go out there and day one they are running the show and it is just not reality, no other profession does that.

SHARNE: You might want to talk, maybe a phone interview with Lane (my brother), he also did his doctorate or thesis, he spent 12 years studying something similar around this so maybe he can contribute to what you are doing.

MC: The other thing I've done and you said that before, if you at taxonomy of knowledge areas because on its own this means nothing, there's two ways I'm doing this, first of all I'm looking at how we present it to people and then how we present it to graduates. One of the arguments they say, when they look at a domain such as this it is based on what they call hierarchical relationships so some things are subordinate or superordinate to others, this comes out of ethnographic research so when they look at a merging domain the knowledge categories themselves and then they look at their relationships so this led to a final diagram and this is dynamic. One of the other guys said some of it isn't linear and later on I'm doing an MDS questionnaire where mathematically I might take 35 of these concepts forward and they will all be related to each other so mathematically we will get this grid where the summation of everyone's beliefs are where things are related they will sit, the first thing they say is they should have a greater understanding of the connection so the hierarchy so the concept of security sits above everything else and then imbedded under that is the notion of law because security has to comply with the law and that sort of thing so what this leads onto and this becomes a heuristic, so we will be able to say to students here is a the physical domain, here's the knowledge categories so we learn about threat and risk and systems and CCTV and access control and here is how it fit together. It's the same thing, a lot of graduates don't know how to employ what they learn, they don't know how to integrate new information with pre-existing information, they don't sometimes understand why they are learning something. For instance if someone did four weeks of electrical security and they are thinking I'm studying security what am I doing electrical security for. Very quickly when you look at something heuristic like this you see that electrical fits in with technology and if you don't understand how basic switches and that fit together and operate.

SHARNE: I think that is an absolutely must from the graduates we see.

MC: For my thesis I'm looking at what are the knowledge areas or categories so do we need to teach threat and as part of that risk do we need to teach system design or CPTED, what are the knowledge categories and how do they fit together so we can say to people well this is why you need to learn this.

SHARNE: I can give you some practical examples of areas that just come to mind, if I compare myself and what I was equipped with coming out of university from the degree I did versus some of the engineers and graduates that I work with. One of the big gaps I see is, rightly or wrongly because of the structure

of the course at ECU, most of it was about report writing so I can write a report and I can analyse an issue and I can to a conclusion, I can draw something that is grey and come to what I believe is a logical approach. One of the whole things around security is, particularly when you are dealing with engineers every day, there was that whole debate to is it an engineering discipline or is it a science, and I firmly believe it is a science, and one of the issues I think engineering firms struggle with is the first thing they come to us and say where is the standard that tells me how to do this, and when you say there isn't a standard and the answer is I believe this, they struggle with that concept because everything they do comes out of a standard, and as long as they are within the guidelines of those standards then they are okay which then relates back to what you've touched on already in terms of if you don't have the theory behind you in terms of how to analyse risk, how to analyse threat, if you don't have the knowledge of how security operations security management work, again you haven't looked at the risk and you can't analyse a problem then you will never come up with the security solution because you can only see from an engineering point of view and we come across that daily with some of our engineer graduates where literally until it is at design development stage where all the concept and scoping have been done and you give them a problem and say right here's the problem this is the solution or come up with a solution to this, not a problem. Go away come up with the schematics, come up with a design – done. But give them that initial problem without all that background and without having solved we believe the solution should be and they just look at you and can't understand what am I designing and another thing they cannot write a report. Engineers cannot write a report. So I map all of this back to, ironically when I did the degree my background comes more in the analysis risk and threat side, I had to learn the engineering, I've ended up in a role in the job where design and engineering is primarily what I do and I had to learn that on the job but I think it works, I can do both, I look at the engineers and they come up with a wonderful CCTV design but if you ask them why the majority of the time they don't really know.

MC: One of the guys in my focus group said is diagnosis, at the end of the day we can get an engineer to build a wall or we can get an engineer to design a system but if they don't know what they are designing then they are useless in terms of the solution.

SHARNE: Absolutely, fundamental to being a physical security practitioner.

MC: When you talk about engineering design, one of the things we have struggled with for example, I believe that students should know the math that sits behind it, when you are designing a CCTV it is based on a field of view so you need to be able to calculate that field of view. When you look at structural resistance to force so if we say the threat is a truck travelling at 80 kms per hour 2.5 tonnes, we need to understand the structural resistance to that in terms of threat. A lot of people say when no that is the engineer's role, what is your position based on your experience?

SHARNE: I think that comes down to the philosophy of that particular professional or practice, we like to think that we do here everything from the risk, threat assessment scoping, through to the detailed engineering. Having said that if you are talking about vehicle ratings and vehicle penetration testing, I'm not

	a structural engineering so we would still engage the requirements of a structural engineer to do relevance of that but we would like to think the security consultant has been involved with and carries the design through all the way and doesn't rely on a structural engineer. So in the designs we put forward the security take the lead and they seek input from engineers, architects etc. to do that. So I suppose yes is the answer to all of that. Other consultants are different, plenty of consultants that are out there and call themselves physical security professionals, and in some cases their primary role, and a lot of our clients can be that way, they will do the initial risk assessment but when it comes to technical design they will get somebody else to do it, that is for professional reasons, for commercial business reasons for a whole range of skill limitations, there are other consultants that will do a design up to concept level and get the contractors to design and do all the calculations and all of that. I don't think that is the right way to go, if it is a developing profession which it is we should be setting up training and educating our graduates to understand all of that information and to produce with all of the calculations they need to do whether it is designing a CCTV system or understanding the broad calculations for vehicle and bollard protection. But you are right you need to be able to come to the point to understand you are not a structural engineer, at some point you expose yourself and the client if you believe you are. That was the other point I was going to make earlier, there are people who will consider themselves a physical security professional but under physical security they are talking in the risk threat assessment sphere. So when you use the term physical security professional are you also considering those people who do more risk work and don't actually do the design.
WAYNE & Michael Coole	
WG:	So all these in your research are a part of the banner of physical security.
MC:	We have the concept of security itself but we also have things like CCTV. With systems, what came out of my last phase of the study was that it more relates to systems theory and the principles of systems, so different security systems, for example a push bike, you can have a very expensive pushbike or your Kmart cheap pushbike but they are both systems. So security is the same, if you look at the security for a domestic dwelling even a higher level domestic dwelling as opposed to a prison, they are completely different. So the argument was that the notion of a security system has to sit within the principles of systems theory so that systems theory becomes one of those categories that we need to teach. Things like keys, barriers so they are sort of areas that have emerged that security professionals need to be abreast of and one of the things I am trying to work out is, if you look at an alarm installer, a security professional doesn't need to know how to install the alarm per say, but he needs to understand it, but his role is not to go there and start wiring it up, same as locks, he needs to understand locking systems principles but does he need to be a locksmith.
WG:	No, but it is a fine line I'm finding especially, otherwise you can have the wool pulled over your eyes to such an extent that you rely on the guys in the field, the contractors and if you don't know exactly shouldn't those wires by

the other way around because you are not doing the monitoring back at the system like the system says it can do then I assume it's doing but it's not really because you haven't actually done it like that. It's a very fine line, a lot finer that I thought it would be when I first joined if I'm honest. The ability to have to know and look in a rack or cabinet and see what it all means is a huge learning curve.

MC: If you look at CCTV it's a knowledge area in of its own right. And so the question is when you start to look at the depth and breadth of just physical security, what is it that we need to know and more importantly for education what do we need to teach?

WG: One of the main ones that came to me, I guess coming from Uni straight into, I guess this is my first job, was we never did anything with engineering drawings, that was a huge learning curve.

MC: I think you are spot on there, in fact one of the other participants said things like engineering drawings and you will see there that it is not a category that is actually on there.

WG: Yes and while I wouldn't attribute it to physical security per say I guess we have a unique view of physical security, we tend to see that more as your barrier type things, things that aren't electronic essentially. And while we see they are a major component of security holistically the management of physical and electronic, there would be a whole lot of things in here that if asked would you see those as physical security we would probably say not particularly no, like CCTV for instance.

MC: So in terms of that is there any lines that you don't understand?

WG: Facility contextualisation, what does that refer to?

MC: In the American language they use the concept of physical characterisation, understanding the facility, so if we look at a prison, well this is Casuarina prison it's a maximum security prison, what are the threats that propose a risk, how does it operate. The argument is universities have their own characterisation. In the extracted terms facility characterisation came out but all of the other experts that I interviewed, they said you still haven't captured context so the security context sits above everything, so trying to understand and trying to get a word or term to actually captures context was very very hard. We ended up merging facility characterisation with the notion of context so contextualisation so what is this facility, what does it do, how does it do it, why does it do it etc. Understanding –if you don't understanding that facility you can't understand the threats that propose a risk and therefore diagnose the problem and look at treatment. It is a sort of combination of Australian vernacular and American language because most of the books are written in America.

WG: But otherwise yes. There is nothing on there that I don't understand otherwise. I need to get my head around the fact of when you are talking about physical security you are talking about security as such not barriers and bollards and walls.

MC: When we are looking at physical security, if you look at a system device or practice of a tangible nature in terms of stopping someone, and I use the word control and you see control actually appears there, physical security is about control, so you look at a physical protection system for a prison it's about controlling the ingress and egress if you look at the environment even

here you still have physical security and what we look at is technical, physical and procedural elements as they couple together. That comes out of trimbox so it's a category within the security risk management body of knowledge and as I said its separate to security management so security management has connotations of management of supervising people so for example in your role you wouldn't be supervising guards, you wouldn't be writing up duty rosters, you wouldn't be budgeting, that sort of stuff and from a jurisdictional boundary that does become the area of security management. One of the problems is how do we articulate a course, someone says I want to become a 'security manager' and I have had to do this, I say you need to go to management school and do these three units in management theory. What I've found is we talk about security professionals and it's become this globalised term and we are finding we are capturing people who focus in terrorism, fraud prevention and a lot of them come from economic back grounds but are still security professionals per say. I'm looking at the diagnosis and treatment of physical access, say you look at a supermarket, they might have some physical security and all this is captured in it, some people say it is really an engineering degree, but it's not because I've got engineers and they say they know nothing about procedures they calculate physical resistant to manipulation, stress.

So do you agree in principle with most of it or do you have any you don't agree with?

WG: Coming from the angle you are coming from I don't think there is anything that I don't. Maybe security surveys actually, where does that fit in from a physical security point?

MC: If you look at a lot of the books on security, once again they are very American centric, they talk about security survey conducting an analysis of the facility, understanding its threats and vulnerabilities and then reporting on those, they talk about security surveys, door locks, are there door locks and it is looking at the whole facility so you look at Casuarina and they say we want you to do a security survey, and I always believe they are contextually, a security survey for someone moving from the inside to the out is different from someone moving from the outside to in for assistance as different from someone trying to move drugs around internally, they are very contextual. The idea is that it's an inspection of the whole process so textual, physical and procedural. One of the guys actually said devices, he seemed to think that the word devices because it covers alarms, access control, automatic bollards and all that, he said you captured those and questioned whether you needed the word devices or whether it is an over-encompassing term.

WG: I can see where he is coming from. Couldn't think of anything else off the top of my head that I would put in there additionally, I think most of it is well and truly covered.

MC: Just the one you said before, things like engineering drawings. That is a knowledge thing, and one of the questions I will be asking my focus group is what do you need to learn prior to graduation of any course and what do you get on the job training. I mean at this stage the depth comes from on the job.

WG: Absolutely, you learn terminology and things like that is mainly what I've

found coming into it. I'd say the majority of what I've done if I looked at it, you've got some mock up assignments how would you secure this facility or how would you do that and when you look at how you would actually do that now having been in industry, it is actually quite different to the theoretical component of how you would do it, with unlimited budget and letting your mind go.

GARRHETT & Michael Coole

Michael Coole _ Garrhett

MC: What I've found is the jurisdictional boundaries, we talk about security professionals, no one really has defined that security professional, if you go to Australian Bureau of Statistics there is no job listing for a security professional, there's engineers, there's alarm installers, locksmiths but no and one of the things I've found is that knowledge is separate. When I was at justice, managing people, that organising, planning, leading, controlling, staffing, budgeting they are completely different knowledge skill requisites to diagnosing. What I've found so far is when we look at the physical security professional or consultant, or protective advisor the knowledge is based down of this concept of diagnosing the problem, inferring or reasoning about it, in terms of understanding it and treatment. That comes from medicine, they diagnose, they reason and they work through the process of exclusion where they try different things and eventually they will have a diagnosis. In security we can't necessarily exclude, they do that in safe manufacturing where as someone beats a control they then adjust it, but security we construct the problem, so we diagnose by construction looking at threats and such that. What I've found is our knowledge is requisite based on diagnosing the problem in terms of physical security or access control and it's about that broader concept of control and treating it but not its ongoing management that is the area of security management. You are not worried about writing staff rosters. I remember I would spend a whole day to cover one shift because you ring up five guys and they say they don't want to work. That is security management whereas what you guys do is very different.

Garrhett: Operations and consulting

MC: It's funny you said things like policy, this comes to what I've been doing, policy has never come out of it. One of the arguments is that the experts write the text books, and the more something appears in a text the more salient it is within that domain space so I reviewed 15 security text books and I did a count analysis on every word and then I did kick words, then I got the top 49 words from that extracted text, so I did that 15 times and then added it all together to get the top 49 of all the extracted text and that developed this table here and what this is is a combination of broader concepts, some core knowledge such as CPTED and CCTV, and some what they call professional skills or enabling skills such as writing reports and things like that. Now this is based on the argument that for me physical security is a cultural domain and it comes out of ethnographic research and they argue that a cultural domain is based on a single semantic relationship with its cover term which for us should be security and luckily for me when I did the count analysis that is what came up. So these are organised based

on how often they came up in extracted text.

Garrhett: Did you have a look at how they had defined these terms?

MC: Yes, the synonymous terms was the biggest headache I've had in this study so far and what I've had to do is look at different definitions across different text and I went through a synonymous term merging. What I also had to accept is that it can't be perfect, security uses the same words in different ways.

Garrhett: That is something that we do as well, when you say physical security for us we are talking about walls and bars and gates because when in an engineering context we have got elec technology, we've got operational and physical, so that is how us as a firm, and we communicate to our clients, I think that is quite common in consulting or engineering practice for security consultants. Regularly in a proposal we would say we could advise on physical security but would have a structural engineering design it for us.

MC: Yes and if you say protective security people think about policy, procedures things like that as well. What I had to defer to was how the text books define physical security, so device system or practice of a tangible nature in terms and even that, I saw on Linked-in that all these jobs for physical security professionals and thought what is that, that is what my thesis is about – what is a security professional generally and what is their knowledge and more importantly, this is not security thesis it's an education thesis.

Garrhett: That was the same as my security research program when I did my bachelors, when I did my undergrad I did an education one, the taxonomy of education was my underlying theory, that was a while ago so I know where you are going from – you are doing it for security but you are in a different domain.

MC: I'm going to get senior guys together at the end and run some focus groups, show them this is what we've come up with and here are the two different knowledge structures. One of the things that the table is based on the argument that the knowledge is organised hierarchically but I'm doing a mathematical one and multi-dimensional statistical scale – an MDS map and that's because it is not all linear so that will tell us how every concept is related to every other concept and so it will be what does this mean for education.

So what we have here is just those top 49 categories and I guess the first question is, is there any that you don't understand or anything you don't agree with, some of them are concepts like control, the argument is that physical security is about control so it's a broader concept so things like defence in depth help us achieve that control. Things like system, in the pilot study it came out that when we talk about systems as a concept is different to alarm systems, systems theory is the overarching theme that people need to know.

Garrhett: Do you have this defined.

MC: Some of it is defined, one of the things I'm going to have to do is try and go through and do a clear definition, some of it comes from engineering, so if you look at structural strength that is an engineering term not a security term.

Garrhett: For me to say yes or no I agree if I have system in here is what you mean by system but otherwise I'd say system is not too important, but look it's come

second on the list has it?

MC: Yes and in fact every text it came up first initially so the notion of systems, if you look at Mary Lynne's books and things like that the physical protection system is what they refer to.

Garrhett: I don't know if you've heard of, It was originally the Kieran triangle and that is basically our system when we are talking and when we have added in a cost benefit so it is more like a diamond now because we try to sell that to the client as well but that is basically our approach, that is our system, so I can see where systems would be.

MC: That is one of the things that I developed, when we took the Kieran triangle, we had security risk management up here that was the systems driver and then the system you had the technical, your physical, your procedural and your management in the middle and what we ended up with was this sort of triangle where these are all interrelated, we did this for a critical infrastructure text. So security management sat within here in terms of managing the technical, physical and procedural and so you had threat sitting above here, so where you had threat and then you had intent and all that sort of stuff, this was T4 model, so then this was part of your monitor and review and so the idea was that system was driven top down, these were the operational variables but this was relating to decay, but decay in the system occurs from the bottom up so the decay at each of the constitutes represents a decay and risk treatment. So that was an adjustment of the Kieran triangle.

Garrhett: I think one of the issues that we have in risk management is that it is important to say that decisions are based on risk management etc. but it is hard to oversell when you have a new client because sometimes it can come back to bite you, they might not have a budget for risk management, they might not have an appetite to do a risk assessment, even though as security professionals we know steps risks need to be taken. You talk to a layman and they have a budget to just put in cameras and if our proposals or if our approach is so risk based we can actually lose the work.

MC: That is a hard one because not always the controls, if you look at CCTV it doesn't necessarily reduce risk.

Garrhett: Yes they've just got that in their head. We find that a lot, compared to Dubai, I'm finding that more in Perth that we will go to a client who will say we want a security concept plan and we have to go in and sell the fact that, look you haven't asked for a risk assessment you obviously don't have a budget for it but as part of our concept we are going to do a brief one for you and we have to very careful about not over committing to the risk assessment because that can become a huge amount of work and we just have to list a couple of things for them. Whereas in Dubai they had a very clear process, the guys up above were basically you need to do a risk assessment and it was just part and in ground into the whole construction process so it is very easy to go in and just do a risk assessment and then base your design off it. Out here, I've heard guys say risk assessments are a black art, it's like well they are really important they are not really as big in Perth as I've found in other places.

MC: People expect you to come and say here's your problem, now here's your system, they don't want to pay for that diagnosis.

Garrhett: Sometimes we get engaged by security managers who already think they know, I don't know if they've done an internal risk assessment that they don't show us or they believe they already know how to fix it and they just engage us to design it.

MC: That is part of that overlap, some people say they know what their vulnerabilities are. I had that in Laos, I did a job on a gold mine and they said we know what's wrong we just want you to come up and recommend some stuff and when I got there I thought you had so far missed the mark and they were talking about technology and saying they want this and they want that, I was thinking this place is in the middle of the jungle, the technology they had was so decrepit it wasn't working and they couldn't maintain what they had, do you really want more technology. Their biggest vulnerability was they had no comms, we said if you want to increase security put in a communications tower and increase comms across the site and we divided the site up into sectors. When we went back he said that was gold. Most of the stuff we recommended was CPTED because they couldn't get the maintainers in the jungle to fix technology.

Garrhett: I can understand that, is the technology available and maintainable.

MC: So with this what I've had to do, some of it is very operational such as lens, the argument is that this knowledge is therefore organised hierarchically so some things sit super ordinate or subordinate to others and all this is a way of trying to organise knowledge because this is a random matrix based on how they came out in the count analysis so I had no control on how this table was ordered. This table has tried to order it hierarchal and this leads to this graphic heuristic so the argument is this comes from cultural domain analysis, what we can have we can show how different knowledge is related to other knowledge, so for a student you can ask why am I learning about technology, why am I learning about delay, how does response fit in, how does risk fit into design and planning, so the idea is that it is just a heuristic to say here are the knowledge categories and this is how the domain knowledge fits together. What we've found is professional practice based on diagnosis, inference and treatment in this the diagnosis sits at the top almost and the inference and treatment sits coming in under that. My first question is, if there isn't anything that you don't understand, but also do you think that there is anything I've missed or shouldn't be there based on your experience as a security consultant?

Garrhett: I was going to say management in general.

MC: I actually kicked management out, and the reason for that is in the text management related to security management so you've got that jurisdictional boundary issue so there is a difference between what you guys do here as opposed to someone writing management rosters, doing staff wages and all that.

Garrhett: I agree. Project management is definitely, having said that though I guess I know the security management masters does touch on a little bit of the operational side but I could do the actual research in something completely different but to have that security and management thing on my resume is huge for a corporation like this.

MC: What we have been doing now is we say to people what is your focus, for instance I have a number of students from the military doing that and I get

	them to do three units from the management school, from the MDA program because they want to be managers.
Garrhett:	Even if I did the masters, completely in a technical side, I'm still going to have management, and that is what they are going to see, they are not going to know what units I have done, they are not going to know that it was completely technical but just being able to have masters in something, whatever management that is going to tick boxes for them.
MC:	Funny you should say that, I did the MSc and people don't understand it, well Master of Science what does that mean.
Garrhett:	Well mine will be a Masters of science still.
MC:	No, well it depends, you can either do a Masters of science or Masters of security management, there are a lot of units that are similar but a Masters of science is like this, you have to go do a thesis, with the masters of security management it is course work. At the end of that you do a project.
Garrhett:	Having that management on the end is basically going to
MC:	But you're no longer a graduate so when you look at this I'm saying what does a graduate need, it might be a Tafe course. You are at the stage now where you are leading a team.
Garrhett:	Yes I'm at a higher level yes.
MC:	The next lot are your skills, one of the things that came out, you have sort of a triangle, you have graduates here, competent professionals then as you go into this stream you become a manager or a senior partner type role and that has a new stratum.
Garrhett:	I'm not sure if you know Clinton Flowers but he is our Operations Centre Manager and he came through security so he was defence and then he worked as a security consultant in the Sydney or Melbourne team and sort of went up and now having someone who has come from security, because a lot of these managers don't understand security, but having someone who has come from security it is now so much easier to do business and get proposals and get some insight into how the business works and applying it in a security proposal is so beneficial.
MC:	It is interesting you say that, one of the arguments, this came out in my focus group, at the end of the day it must be a degree level outcome so there is no reason why graduate security program can't be a CEO. We are looking at developing the same attributes, the core knowledge is different but we are looking at developing the same graduate attributes and that is why things like report writing is very generic, things like analysis and evaluation. It kept coming up in the word extraction and everyone said that is the most important thing, if you can't analyse a problem, if you can't evaluate it and communicate your analysis you are worthless.
Garrhett:	I guess there is a huge amount of things that are cross domain that the course still needs to deliver, we are just looking at the course security stuff here?
MC:	I'm look at everything, any of the attributes the core knowledge that you think is missing from here from your perspective or any professional attributes that you think are missing from your perspective because all degrees are based on core knowledge and what they call graduate attributes.
Garrhett:	So these standards and network policies are different ones, you've got standard and networks.

MC: Things like standards kept coming up and understanding different standards. Things like networks and networking if you look at convergence now it is becoming a big issue for physical as well, but things like broader issues such as infrastructure. One of my other experts said if you don't understand infrastructure, what I also had was a number of guys say some of the other experts talked about things that were missing, things like understanding structural strengths, we look at CCTV but a couple of them said things like surveillance you need to know the broader concept of surveillance first and then the CCTV achieves that. Things like movement control, so electric power, situational crime prevention because a lot of physical security really is situational crime prevention its context driven stuff.

Garrhett: I had this discussion with Dave and Jeff before about the graduates we were getting in they didn't actually know what we did and I talked to them about writing a module or a minor in specifically tailored around consulting because they were coming in with the theories of CPTED and things like that but they had no idea of the process that we go through about obviously there is the proposal stage but all the way up to commissioning, like writing the design brief, doing the detailed design, what are the different stages you can do, a concept or a master plan and then you do a 50% design then you have a 100% design and then you've got reviewing shop drawings from the actual installers and then you've got commissioning and things like the fac test, the factory acceptance test, so all that process is really beneficial to already have an understanding of because even if you are not a consultant like us but if you are working in a firm you are will be communicating at that level, if you are designing a system yourself and then engaging the sub contractor yourself, you are still going to go through that process.

MC: One of your other guys said project management and one said understanding the project scope, another said the basic fundamentals but would you see that sitting within a broader unit of say project management, the design process or would you see it as separate?

Garrhett: I think if we use the word project management we are talking about likely operational security side, suddenly we are talking about the operational project management side, getting the resources, do we have the resources to do the project, what are the timings etc. I'm just talking about the process and the different processes, there is another one called FEED, which is Front End Engineering Design then there is EPCM Engineering Procurement Construction Management, and we have to deal with all these different processes that do share similarities but also differences and fit in our program and what we do into that and what the client wants.

MC: So where you've got that category planning and design, and that is represented up here, would you say that that would be able to capture it in that broader heading of planning and design.

Garrhett: I'm not sure, because planning and design for us is when we already have the program and we know what we are doing and it's inputting security into the early stages that is what we call it. How the client is planning on achieving the project is different I think to that up front planning and design because we already know we have a master plan and we are going to be in charge of procurement and we are going to be doing x, y, z and now we are saying alright guys you are going to need this many pipes or conduit or we

are doing a blast analysis and it's all that really upfront stuff, whereas I think having an understanding of the different engineering processes that we have to go through could be beneficial. Have you done a EPCM before or a FEED?

MC: Yes, they are completely different.

Garrhett: And they are different across different industries as well, if you do a FEED for resources and power and do a FEED for the built environment they have different gates that the project has to go through so they have different drivers so I found that really interesting. So you are applying your security knowledge and then you've got a different industry and they treat the process differently.

MC: How would you capture that as a knowledge area or category, what word would you use to describe that?

Garrhett: I will have to think about it, but is like engineering practices. It is consulting processes or practices. It leads to different responsibilities for the security professional and EPCM, so we've got engineering procurement construction management, not only are we doing the design of the facility but we have to manage the security of that facility while its being built and now with Jacobs who do a lot of EPCMs, they can put in a guard force and manage the security after its been built. We are looking at an EPCM in Mongolia, its already an existing site and we are doing an add on to it, so we have to design the actual physical security, which is all the electronics and everything, we have to write policies and procedures to fit in with the existing site and then manage the guard force that is going to be there. It's opened up a whole new world of consulting to me, we only really looked at from one aspect to it, and now that Jacobs is on board we have opened up a whole new brand. It would be interesting I could give you probably more information on what our role as consultants would be in a year or two when I know myself.

MC: Yes because managing people is different again, at that operational level.

Garrhett: We used to sit in a built environment which I don't know if someone has explained to you the structure that we had here but we had water and energy, power and resources, buildings and infrastructure, within buildings and infrastructure so that was roads and buildings and all that infrastructure development. Buildings and infrastructure was split into infrastructure and then built environment and we used to sit with the engineers, we used to sit with the mechanical, electrical and hydraulic engineers and we were security engineers even though we didn't have engineering degrees we sat with the guys who fit out a building, now we've been taken out of that and we sit in strategic consulting, so basically we are able to do not only work for clients but also internal work for the company, so when they are going overseas we can do the risk assessment for their travel plan or their accommodation that they are staying in, I'm actually flying to Saudi Arabia to do an assessment on accommodation and the office building and give them treatment options to upgrade it or whatever my findings are but it's not just become an external resource we are now very much so an internal resource as well for these larger EPCM projects. I'm not sure if in the future that might mean taking on operational managers as well but if you look at consulting as HSSEC – so health, safety, security, environment, community;

we are now more and more fitting into that brand and we have internal health and safety advisers and they are now also going to be looking externally, so when we have one of these EPCM projects, not only are they doing the health and safety and policies for Jacobs but they'll be writing them for the client.

DES & Michael Coole

Michael Coole _ DES

MC: You've been in the industry and working as a security consultant for a long time, what I'm looking at under this concept of the security professional and nowadays its physical security professional, so that takes in consultants such as engineering companies and in-house security advisers, what is the knowledge a graduate needs and how should we teach that, make that generalised education. What I've done to date is, the first argument is the experts write the text books so the knowledge is gathered in the text, what I've done I've gone with 15 of the most common or broadest knowledge text for security so I looked at the ASIS body of knowledge etc., the argument is the more something occurs in the text the more it's a salient theme in that domain area so I did a count check analysis of all the words and terminology in all these text, I did that for each text and then I combined it, I ended up with this table here and what this table is a combination of broader concepts, such as security as a concept and control as a concept, core knowledge areas such as CCTV and things like general capability attributes say professional enables such as analysis and evaluation the ability to critically evaluate something, communication skills, the ability to write a report. So what I'm looking at first is if I can show you the table, the first one has the raw knowledge areas and these are not in my order, they are in the order that the occurrence occurred, so things like electrical power, the concept of interruption so I'm looking at a physical protection system. What I'm looking at is if there are any areas you don't understand but also what do you think it has missed? So the text books haven't covered everything, is what I've found, so I'm asking people like yourself – here is what the text books are saying in a broader sense, but what have we missed?

DES: So these are words that you've basically, these topped the word count? It does a pretty good job of picking up a lot of the key points, some of them are there because they are common words and probably not as important but in order of the others its pretty good.

MC: Some of the things that some of the guys have said are things like engineering drawings or project management are missing. What I also have with this table here, these are some of the things that some of other experts have said, things like broader understanding of situational crime prevention, defence in depth didn't come up in the word count but I've added it, that is the basic table and from the basic table I've added these ones here, I guess what I'm asking now is there anything that you think is missing or shouldn't actually be there.

DES: I don't know about things that shouldn't be there, one thing is infrastructure is a very broad term, so certainly from my perspective a couple of things that aren't and knowing where I come from in terms of, I was looking for

the word management.

MC: Management, interestingly enough – Garrhett said the same, I took management out of the count check because security management is different to what you guys do. If I'm looking at physical security say looking at advise system or practice of a tangible nature, say the knowledge of someone who is managing security say Royal Perth Hospital or Casuarina is different to what you guys need to do, they argue that the knowledge is based on three elements of professional practice which is diagnosis, inference and treatment. So for us it's about diagnosing the security problem and reasoning about to set the level and actually designing the system but its ongoing management in terms of operational sense is the area of security management, so in order to bound my study I've had to say security management is another sub domain.

DES: When I say management I'm talking about the management, not necessarily of the security but maybe the management of, from our point of view, management of process and that is management of process in terms of what you do, your study, but also management of process in terms of a working environment because it becomes quite important to a grad to understand that you come in and get given a job and the management and the process of delivering that job is something they need to learn. There is a point where a task, we write a proposal, we win a job, it lands on someone's desk it's the management of process of understanding how I get from the point of having this to actually achieving the deliverable.

MC: Garrhett said something similar, one of the things he said he was talking about the process from the bid right through to when you get the job and then how you design that but that is different to project management in terms of project managing is about the operational management of that project, how would you capture that as a knowledge area?

DES: I'm being very careful because I don't want to wrap, Project management becomes a much broader issue than what we are talking about, we have all these things in here that talk about technology but if you're talking about teaching someone the education process of how to work in this industry there is a general process around, you are going to be working either for a business or for a client, you are going to be provided a service in house for that business you might be employed by BHP on the security team and you are working in there or you are working for someone that is outside providing that service to that organisation. Either way at some point you are given a project and there is a process and there is a way of managing, I suppose it's almost around time management and understanding how to achieve a deliverable, it's really difficult to put some wording around that. I suppose I'm just leaning to you can know and understand all these sorts of things, if you don't know how to, it's almost like you give someone an assignment, how do they plan and managing the delivery and the output of that assignment. In itself I think it is something that, it is being able to get that context around what it is your being asked to do, understanding from the early days of what is the key point, what are the deliverables, you do not run off and do what you think needs to be done but actually delivering what you have been tasked to do. That in itself, from a security point of view, is absolutely, because if you haven't got the context and don't understand the

task we end up, the other word the term I use a lot its around mitigation, security is around what we do and have I achieved, we talk about mitigation strategy in the end we want to look back and measure and did we actually mitigate that risk, did we actually achieve what the client needed done. I put it in the context of sometimes people will write a proposal for a job and quite often they will write and tell the client, I'm really good at doing this and we are good at that, but what they don't do is they don't actually look at what they've been asked to do and address that; actually have we offered to do that for that client, have we attributed the correct people and skills and management around the process to actually get to an outcome, at the end of the day when the job is finished no matter how many gates we go through but we've actually delivered to them what they've asked for.

MC: So you are looking at what is the objective, do we understand the objective?

DES: Yes, do we understand the objective, do we know how to plan to achieve that objective, do we know how to implement the process to achieve the object and do we know how to deliver it. To me that is a really important thing coz otherwise you can quite often give a person or client an outcome that doesn't necessarily meet their needs. It's a bit like, if I have a person with a security issue and if you sat down at a table and someone said we should start talking about cameras here and access controlling this door and I'd sort of go well can we move the plan out of the way, can we talk to you about what actually is the problem, it is caused by what risks, what's your threats and risks. So going back to understanding, you get an outcome that delivers on that.

MC: That is going back to those attributes, what they are arguing in any profession so whether it is medicine or law, so law they diagnose a legal problem and then they understand establish a plan to treat that to argue their case. Medicine is the same, they diagnose a medical ailment and then they treat that, not the surrounding ailments and so the argument with us is that we should be diagnosing a security problem and then treating that problem.

DES: Its then understanding if the problem has been diagnosed then what's the plan, so your doctor might say well we not going to put you on aspirin because your blood is already thin so it's a matter of how do you interpret, its understanding the process that you need to go to, to interpret that evaluation and know how to plan the way to get to the point that you have got the correct treatment process in place and therefore you get the desired outcome.

MC: And it's hard to capture that in a category.

DES: In terms of this it is the sort of thing that throws that together, is that too overarching to be useful to what you are looking for.

MC: Not necessarily. The other argument is, students in terms of how we code information, so if you give them all these knowledge as a matrix and say learn that, they don't understand what they are learning and how it fits together. This process came out of what they call ethnographic research, where you look at how a culture is related and they argue, one of the ways a culture is related is hierarchical and what I've had to do is develop a hierarchical table and then map that to a figure like a graphic, so in theory the students should be able to see the knowledge they are learning such as crime prevention or understanding risk management and security risk or

planning and design and see how it fits in with other knowledge and then they can up and down the depth. For instance one of my other guys said CCTV, you've got it as a knowledge category, he said all security people need to understand CCTV but in reality that has its own body of knowledge it's a specialisation in and of itself, you have people that just specialise in CCTV and so he said in terms of what is your depth and breadth we don't know, yes you need to know CCTV but you can't be an expert of all this.

DES: That is actually a really good point and if you take that example of CCTV, do I have the in-depth technical knowledge that an installer would have of pics or a digital camera and the way it forms, absolutely you wouldn't. Are there people downstairs in our security team that know more about the CCTV performance than me, absolutely, so in each one depending on where you are sitting and what you've got to do, the depth of the knowledge – I think that depth and knowledge is depending on the career path that they go to. It's a point of educating and giving enough information that allows that person to understand the whole of the industry and therefore make decisions about what they want to do and where they go in terms of a career. Not only that it also allows them when they are in that career path to know what they don't know and know how to get access to that knowledge.

MC: One of the diagrams I've come up with is, you've got this security professional there and underneath that you have locksmiths, alarm installers and all these operational people that actually do, they achieve that – you've got fence installers and stuff like that; and so the role of the security professional is to bring that together to achieve the objective that you were talking about. An alarm system on its own isn't going to achieve security it's a physical protection system. So you have this security professional but they also have to liaise with other professionals, whether it be engineers and stuff like that.

DES: Let's just use that as an example, let's say we are talking about a secure fence, I as a security consultant will talk to our client about the type of delay we need to achieve by that fence and we will define that in three ways - under, through and over, simply as that. So each one of those has to be treated, the through bit is, but it still has to be physically strong enough to withstand the environmental conditions that it is in, whether that be wind, lightning, whatever, so you've got your structural engineer and your civil engineer, they become critically important to the design of the fence. You've got your fence manufacturer that has product that you want to use and understand that. So what I see, we set a criteria around the performance of the fence, I want the face of that fence to be anti-scalable, so I will talk to the potential architect or the person that is designing the fence about how we achieve that, we know that we want limitation penetration and that is around the fence material so we talk to, we know the fence has to stand up and it either has to have some sort of cowl or topping so from your civil engineer, your structural engineer, your fence manufacturer and your fence installer, all of those sorts of people in here, the knowledge that I need to have is not only the objective of what I want but who do I need to talk to. So in the process I need to be talking to a structural engineer, civil engineer about the ground finish, how do we stop the anti-tunnelling, how do we get the water away for the longevity of the fence, electrical engineer, we've got the

lightening protection issues associated with the fence, the manufacturer – how do we detail so we get an anti-climb finish on the fence so that nice smooth finish and then the installers. In terms of the body of knowledge, I suppose what I'm trying to get to is that I have an objective, my way of knowing how to get to that objective is quite complex and it needs to involve other people so I need to know who I need to involve and at what stage of that process to actually achieve the outcome.

MC: So you need to be able to liaise really effectively.

DES: You need to be able to communicate effectively and liaise but you need to understand, the bit I said before know what you don't know, I'm not a structural engineer I can't design the footing for that, I don't know what size members of steel that I might need to stand that fence up in that particular condition, I don't know whether, are we going to have a piled footing into that post and then put some form of anti-dig barrier either horizontal or vertically into that but understanding the process and who I need to involve to achieve the outcome; when we get someone that comes to that fence that we have got some chance of meeting the time delay for what we need and then when we involve the client, if we want to go through a process of prototype testing. If that makes sense, that is the sort of process in terms of management I'm talking about, it's not the project management, delivering a project because that is a different skill, but it's the design process, the design process becomes really critical because firstly do I have the information at hand, has a risk assessment been done, do I actually know what the mitigation strategies are, do we know what we have got to do.

MC: Its funny you should say that because some things when we tested it, we didn't care how easy it was to cut through them because in theory we controlled the inner environment from an inward out approach what we were looking at was anti-scale.

DES: It is knowing what you are trying to achieve. <tape turned off for job example> Just trying to put that out as an example of what I mean in terms of the process and understanding.

MC: As I said that sort of thing doesn't come out in your text books. When you look at all your text books they write about delay time, they look at technology and CCTV, locks and keys, they are the basic things they write about, what the text books don't give you is how it fits together.

DES: I suppose that is the bit here that I said is that too overarching because it ties a lot of this together but it is that understanding of the process so let's not call it management but maybe it is understanding of project delivery, or outcome delivery. So you talked about there being three points which was analysis and evaluation then you moved on to the treatment.

MC: So you have your diagnosis, your inference which is your analysis and evaluation, treatment, then you have your analysis of the end product as well which is what you're saying, your acceptance to make sure you achieve the objective. The other thing is, I've organised this hierarchically so that flows on so this is just a heuristic so this is something that people can recognise, some of this is hierarchical and some of it is, if you look at analysis and evaluation that sits across everything from law, because you've got to understand the legal framework that you are operating in right down to your facility procedures sort of captures everything, your security

surveys, barriers, ability to analyse, things like report writing sit across everything as well, so the only thing that is superordinate to everything is the very concept of security, what it is you are trying to achieve. So based on what this diagram is, which is really just the organisation aspect of this table here, do you think anything is missing or needs rearranging or reorganising?

DES: One line that really stands out as good not as missing is that to me, the fact that you've got that focus on these different bits. Terrorism, general crime, safety and loss drive completely different, under that line they can drive completely, they might be the same in some context by how they are applied but how they get to the end, they have very different drivers so therefore have to be assessed in a completely different way.

MC: That came out of one of the pilot studies, things like one of the new buildings in Singapore, it has to be completely blast proof because they are really worried about terrorism for the context of the facility, that is a huge additional cost that most facilities.

DES: I like that you do have safety there.

MC: One of the UK trained guys, been out here for a while and just gone back, he said why is safety there, and I said look it's not me driving this, my process is the text book provide the initial framework and then I go to all the experts, and every text book the word safety – you can't get away from it.

DES: It is inexorably linked, you can't talk about one without the other I feel.

MC: And we talk about assets such as people, information and property; and people and safety are entwined. So that is something that just kept coming up. Some of the other people said things like project management and where they sit, one of the younger guys said understanding network technology, networking has become vital now especially for things like understanding CCTV, network fundamentals.

DES: The other one I'd say is understanding application, how you apply or why you apply certain selections of materials and things like that to a project. Another example of that is and this was in a major international prison and we go in and we had gone through four or five security checks to go where we are so we were right on the floor where the prisoners were and we were standing outside the guard station and one of the guys said to us, and all this glazing here it's all bullet proof, I said why would you go to bullet proof when we have gone through metal detectors, search, everything, and he said 'oh well if they get a gun' and there was a guy mopping the floor, he had a steel bucket and I said so you have tested this etc.? I said have you tried smashing it with that steel bucket full of water which is really really heavy, and they said oh no but its bullet proof. The person who had set that criteria didn't understand that vandal proof while it might be bullet proof it could be vulnerable to other levels of attack. Bullet proof glazing by itself is not necessarily going to withstand something else. So right at the start of understanding well if we are going to assess what we need there what are we protecting for, so understanding the application, so in terms of this application what does it actually need to be protected against.

MC: When I did the extraction it was actually facility characterisation, that is the American terms, one of my Australian guys said it still doesn't capture context, he said when I look at this it's all great, it was a lot less defined

back then it was a number of stages ago, but he said I still don't see anything that truly captures context and I ended up changing the characterisation to contextualisation, in the Australian vernacular we understand that. But what you are saying is spot on it still doesn't capture, when you look at threat, threat is contextual.

DES: Making sure that as a student that they understand that process of why do you, we say establish the context but how do you do that and how do you know in that you are understanding the application of what comes from the other side of establishing that context.

MC: You are making the point absolutely clear.

DES: While we talk about CCTV, access control that is all great but people have to understand what that is and to a certain degree you have to let go and say well the certain applications and those sort of things around the technology that we are going to let industry teach you because we don't have the time, actually knowing technically how a camera performs is not as important as knowing in your general life in the security industry knowing these other wider things. It's the prioritisation, it's more important to know the in-depth technical application of that camera or understanding the application of a security treatment within an area, what do you base it on.

JOHN & Michael Coole

Michael Coole _ Pettit

MC: Have you had a chance to look over that stuff yet?

PETTIT: I had a quick read of it this morning. So are these 6 questions you wanted to ask about.

MC: I've changed number 1 around a little bit because there are too many synonymous terms that I merged so I did that over here. What I was going to ask for that one when you look at the 49 thematic knowledge categories

PETTIT: And that is in table 2 is it?

MC: When I go to the questionnaire here it will be table 2 yes.

PETTIT: I was trying to work out which table applies to each, you have just got the table instead of referring to a table.

MC: They are different because of the way, trying to fit all this in, the first table is what I got out of the interviews from the first round and the argument is that based on discussions and knowledge we sort of built. When you look at table 2 the main thing – the first question I was going to ask, because I've change what that is – any of the knowledge categories or concepts that you would like clarified before we begin? An interesting one in the pilot study, the concept of systems, it can be so diverse and that is a problem with a lot these things is that we don't have a security dictionary to refer to.

PETTIT: What about that Australian Standard lexicon of security term.

MC: Lexicon is okay in terms of things like risk but for example when you look at systems, in fact what the pilot study guide said is that in fact relates to understanding the systems theory and what a system is. In terms of many of the areas some of them are self-explanatory the concept of security, CCTV, the notion of control, when you look at physical security what we realise quickly is what we are actually talking about is the very concept of control. Controlling access, monitoring the space that we have got controller influence over. Is there any knowledge categories listed in table 2 that you want clarification on?

PETTIT: Not really, I think they are all pretty self-explanatory.
MC: I used 15 security text books and based on a word count analysis, I extracted the top 49 key security words. Some of them I kicked out such as management because I'm not looking at security management I'm looking at physical security or situational crime prevention. So what happened for each text I got a table and then I put all those tables together and their numerical occurrences and I redid it and then I added it all up. So where you had alarms or alarm systems etc., I combined all those like terms, so this is the top 49 when you look at knowledge areas of physical security so some of these are more concept such as control or security itself, others relate to more physical things such as alarms or locks.
PETTIT: Having a look at table 1, what struck me about table 1 I thought there were 3 concepts that were worthy to go in that. They were utility – it is no good having a product and putting it away in a safe so no one can use it, if the security level is such so no one can use it and there is no utility in the product you may as well not have it. I think something when you are looking at physical security the concept of utility; you don't want to have so much security that you can't, the purpose for which you bought this for is no longer.
MC: That is a good point and that hasn't come up at all so that is a really good point.
PETTIT: The problem that we have in the security is that we don't sit down and have these philosophical discussions, and things get raised in this and it gets into normal put out there and different people start talking about it, but it's not an industry that has these philosophical discussions we are having and because of that things that appear in the text, there are critical things that don't appear.
MC: That is what this initial phase here is about, saying okay we have all these things that do appear in the text so for instance, well it because oh well that is not a natural problem we understand we need to learn that lot but you look at some other and a good example is in the last phase, so the focus group, when I did those as a pilot study all the participants said your ability to clearly communicate your message is essential, without that the rest means nothing but you don't find that in the text books.
PETTIT: Certain things are still to be defined, critical elements and I think utility is one of them. It does get mentioned discreetly.
MC: You are right there, when we talk about for instance CCTV comes up all the time, so it's not hard to believe that is the third highest, next to systems and next to security itself, utility your right it's mentioned discreetly it's not salient, it doesn't come up.
PETTIT: It's taken as read but not necessarily, it's a latent term that is present but not really apparent. So I thought that is something I would offer up. The other two that I thought was fit for purpose. There is no point giving some lock or some sort of physical security thing if it is not fit for purpose. A grill is a grill but it's got a hole in it 92 inches square where you can crawl through.
MC: Are you looking at the efficacy for the context. When you say fit for purpose, are you looking at - because you have two different levels, one of the things that keeps coming up is levels, if you go back to the ..... and five levels of security or a good example is you can buy your Kmart special or you can buy your top of the line. Are you looking at the level of security has to be fit for purpose or are you looking at the efficacy of the individual control?
PETTIT: Probably explain it in this way, yes you can buy safety glasses and they have a sign on safety glasses but if they don't stop chips going through the lens and into your eye then they are not fit for purpose.

MC: So you are looking at the physical efficacy of the component?
PETTIT: Yes, I think that is what it is. And I've got efficacy as well.
MC: Do you think efficacy is covered in, what keeps coming up as well if you go to table 2, is the notion of standards, you know security standards and it is not just security I suppose, you've got wiring standards and things like that. Do you think efficacy is covered in the standards or is it too hidden?
PETTIT: I think it is hidden because when you start talking standards people think Australian standards or a level, I think it deserved being teased out a bit more in its own right. Because it seems to me so many security systems they have in place either prevent you from using, take away utility the product all you have bought to use and you may as well not have had it or they have got some sort of security product that is not fit for purpose, it doesn't work, yes it's a security product but it is not really satisfactory and it might be putting close circuit TV in a bank rather than have a guard on the door.
MC: Effective comes up in the word count analysis but the problem is because I'm only taking the top 49 using a 7 x 7 matrix it did drop off, but in most of the text effective as a concept did actually come up every time.
PETTIT: Sometimes these words are not the right word but we don't have the right word in our vocabulary.
MC: That's why I look at effective as efficacy, as efficacious for what it should do. The problem with that is you look at the levels of security so you've got efficacious against a level of threat, so if you have a low level threat ..... high level threat obviously it is not you need a more lament system and that is part of the issue in physical security because it's about the right level of control for the concept. Cost is another thing that kept coming up.
PETTIT: Cost is one of those funny things, especially in occupational health and safety, the principle is if it is a low or moderate cost but delivers a high result it should be adopted. But then again the fact that you don't have sufficient funds to do something is not in itself an argument to say oh well we just didn't have the funds, we could afford the grills on the windows so that was it. The argument is well if you didn't bring the resources necessary to do it safely you shouldn't have indulged in it in the first place.
MC: Yes it's a tricky one that one. In terms of physical security, so if you look at the physical security of a home compared to a bank, cost is a big driving factor in the difference.
PETTIT: And banks, even though they are not short of funds, they are loath to spent money.
MC: Well a lot of people are loath to spend money of physical security aren't they?
PETTIT: Yes.
MC: Interestingly enough, we will talk about our figure as well, when you look at figure 1, that argument is and this comes from most of the literature. What I'm actually doing is undertaking a cultural domain analysis in physical security and a domain is organised along a number of properties, what the first property is if they are organised hierarchically, and that is where table 3 comes into it, in line with point 9, and the argument is this comes from ethnographic research where the argument is that based on the notion of similarities and contrast you should be able to organise those key areas or key concepts hierarchically. What you actually see here is that the knowledge is based on diagnosing the problem and then interrelated in the next ..... section is inference and treatment and inference relates to the concept of professional reasoning and when I do the multi-dimensional statistical scaling questionnaire and we specifically measure

contrast and similarities as you did with the survey before, what I found in my solution of that that mathematical map that those elements more related to diagnosis were clustered together and those elements more related to treatment were clustered together and those that sat in the middle were more on that boundary between and sat within those professional concept of inference. So the argument is that all professional practices are based around the three principles of diagnosis, inference and treatment of the problem, so whether it is law or whether it is medicine etc. like that. You see that has actually emerged based on the knowledge table so from table 1 and table 2 I have been able to using ethnographic research and analysis tried to organise that hierarchically. When we look at 49 extracted concepts and subordinate concepts, do you agree with most of these; and if not what knowledge concepts do you think any others are missing?

PETTIT: Security itself seems to be a nebulous term.

MC: When we look at a cultural domain what they actually argue, the cultural name is based on a single semantic relationship with its cover term and that worked out well for me, that is the premise that I had to go in the study for, so in order for the rest of the study to make sense I had to come up with, I use the cover term security and then using my review of literature I broke it down into areas of jurisdictional boundary because I'm only looking in areas of physical security, but it still must relate to the cover term, when I did the word extraction, security came up in first place, which is refreshing because that actually reinforces that the notion of physical security is related to the cover term security so although security is a broad and nebulous concept, the thematic concept that come out of these, such as protection from threat and control and influence; ..... so the very notion of security and the rest of the body of knowledge for physical security had to be under that concept of security itself. Which in a way was good, that worked out, perhaps where its changed, if you think the broader cover term security underneath that, and if you look at table 3 you will see more hierarchically under security because security isn't ..... the very notion of law, when I did the count analysis law was actually a fair way down.

PETTIT: I would expect it would be because we are still in an embryonic situation where people are not being held accountable for their actions and negligence.

MC: That is interesting that you say that and you are probably right but when you look at physical security you have to comply with the law.

PETTIT: For instance you decide to design a man trap in a bank, what is the legality of having a man trap in a bank and someone walks into it, even if he is a robber, do you have a lawful right to detain that person. What happens if it's someone else who is not a robber?

MC: I see law as influential with the pursuit of the concept of security.

PETTIT: Without understanding what the law is and things like, take bouncing for instance, there was a case where this bloke/transvestite wanted to go into a female club the bouncers wouldn't let him in, he took them to task on the anti-discrimination and won. That is an aspect of law in the application of security, denying people access to a premises or not. Things like self-defence, how far, concepts of occupational health and safety what does the law say about putting certain requirements on people, controlling under the occupation health and safety you have a duty of care to make sure the entry of your building is free from risk, if you have a man trap in there is it free from risk. Here is an interesting one, Armaguard or someone like that between the cab and truck and back where they are carrying the cash, had some sort of man trap and you could only open one door at a time and it malfunctioned, one of their employees got squashed in

there and killed. Now that is an aspect of the law that has got to be free from, whatever your security system has to be free from risk and I think that this is something, Tooma is starting to put books out there highlighting
MC: Rick ..... has been put a few books out there too in relation to law.
PETTIT: Rick is a bit wishy washy, I think he is missing it. He is on the side of the bullseye where as Tooma is dead centre. Actually he is putting out a new book at the end of the year sometime, a third addition of security health and safety in environmental law.
MC: Based on that do you think any of the knowledge concepts or principles within that table should be removed and why?
PETTIT: When you talk device, what are you thinking when you mean device?
MC: Interestingly, the very concept of devices kept coming up and if you look at probably what you are talking about, if you look at a security device we talk about systems but we also talk about individual devices, we talk about alarms and alarm systems but what about access control devices, pop up barrier devices, man traps is a sort of security device, I guess when you look at devices and you start to look at where the concept or the term device is in the text from the extract, device can be pretty much anything when you look at physical security.
PETTIT: I think it is one of these terms it is probably a throwback, it is there but why is it there. It is there enough to put in but not sufficiently specific enough to understand what it is.
MC: And when you look at where it appears, one of the things you look at, where it is appearing in the text. Look at pop up bollards, well they're a device it's a physical security device, they are a barrier, a pop up barrier and I think perhaps we use devices as almost a cover term and sitting underneath that you have alarms, barriers, access control systems etc.
PETTIT: I think it seems to be a term that is there but not probably right for this table.
MC: So it's more a cover term, principle for a range of things like alarms,
PETTIT: Probably better described specifically as an alarm, bollard or something like that rather than device. Then you have standards, that's fine. Network?
MC: If you look at the concept of network, concept is what they call conversions in physical security so what we are saying now is that physical security professionals of the future have to understand networking principles, basic cyber security principles, because a lot of these devices like building management systems, control systems, they are actually all over internet hub. So the concept of understanding networks is now part of understanding how the system is going to fit together.
PETTIT: I would just add an 's' to that would make it a bit more understandable.
MC: Actually I thought I did do that because in the count check network and networks kept coming out so they become basically a merged term.
PETTIT: Network on itself means, go and talk to Mick, Dave etc., networks means a connection of systems.
MC: That is how I've done it for table 3, if you look at the hierarchically table because network sits next to your communication, technology, intrusion.
PETTIT: In order for network to mean networks you need the context for it.
MC: That's right and that is why I had to go back into the text and go where is it appearing.
PETTIT: Property yes, infrastructure, I think glass was an interesting one.
MC: Interestingly enough when you look at more and more now, security people are

having to come to terms with different ranges of glass technology out there, you have glass protection, when you look at intrusion detection systems, a lot of them ..... specific frequency of the glass that you have, if you look at penetration time in terms of glass, some glass will stand a brick for about half a second and other glass will stand people sledge hammering it for an hour. What we are seeing physical security people have to understand the physical resistance of glass, because glass now, you look at glass bricks, I did a number, a few years ago, did ..... on glass bricks delay barrier in a prison and they withstood two people sledge hammering them for an hour. We are starting to use, especially when we look at the concept of transference security where people want the same level of physical security but they want it to be very subtle, we are starting to see glass design as a barrier as well as a means of enhancing the environment.

PETTIT: Talking about glass that raises another one that goes with utility, efficacy and fit for purpose, and that is aesthetics.

MC: Interesting that you should say that because we are moving to this notion of transference security but aesthetics hasn't really come up.

PETTIT: Whilst you want your place to be a prison you don't want it looking like a prison that then flows into things like quality of life.

MC: What they have actually done, and this probably sits with physical security anyway, they are using the use of terminology, some people talk about aesthetics .....security, extension of CPTED, but it's actually not, if you put a CCTV camera inside the light pole instead of mounting it on the outside, it looks more aesthetically pleasing and it makes the security look a lot more subtle but it makes you maintain the field of view output that you wanted in the first place.

PETTIT: When you have heritage listing buildings where it's got to sit into a context, also you don't, which you want to be safe and know that someone is watching you don't want that feeling that you have big cameras pointing at you. Having that oversight tends to decrease a person's quality of life.

MC: That goes back to some of the very principles, if you look at Jamie Jacobs work.

PETTIT: Yes this is fit for purpose, utility, efficacy, aesthetics, quality of life, it is no use living in a safe area where you can't use what your bought, you've protected it so much you can't use this thing anymore, what you did buy for security doesn't work, it makes the place look worse than a wrecking yard or the bad end of town, you just don't feel like wanting to be in that place. There are the sort of things, utility, aesthetics, quality of life, they are not the sort of things that come up in the terms of security.

MC: You're right and they never came up in the text books.

PETTIT: But again I think that is one of these things that a failure of the industry to have philosophical discussions about this.

MC: What I'm trying to do now, is say what if, and hopefully I will deal with some of this in the focus group, what is it that you need graduates, and I have to be careful with the term graduate, people just starting out in the industry after leaving tertiary qualification education courses, what is the knowledge that you need them to graduate with? So if they don't understand what a system is, and a lot of people said that in the pilot study, this relates to the basic system and theory and you see how the principles of physical security comply with the principles of ..... security. CCTV, what came out of the pilot study – they need an understanding of CCTV, no they don't need to be experts, because CCTV has its own body of knowledge in of itself and in fact what has come up if you look at the notion of planning and design for example. Planning and design, you can do a masters in planning. So each one of these knowledge category areas and the

concept of security it has its own body of knowledge.
PETTIT: Even the aspect of CCTV, in NSW pubs and clubs they have laws as to how many cameras, where you have to be recording, how many frames a second how much data you've got to be. This is where a lot of them don't seem to identify the law, how it is relevant, in QLD there is no law against putting up CCTV in the work place, places like NSW you have to put up signs saying 'you are being recorded' so even for CCTV, it seems that law seems to be the overriding factor there, without abiding by the law you can't install anything.
MC: It is interesting looking at what are we actually trying to draw out. If you look at the knowledge table, table 2, then you go to table 3 where I've tried to organise it hierarchically, the idea of organising it hierarchically was to show how it is connected in terms of structure and then that led into figure 1, and figure 1 the idea is that what we are actually showing is the local connections, for someone who is just starting out in security studies ok and we say okay we are going to learn the concept of risk and they stay to understand where risk fits in to diagnosing the problem, if you look at the notion of technology so we look at detection and technology they go okay this is why I'm learning about technology because technology is a salient aspect of physical security now. So if you look at the concept of movement control and these all relate to defence in depth and defence in depth goes back to situational crime prevention and stuff like that and understanding infrastructure. So if you look at that, do you support the structure of the map or do you think that any of the areas should be moved. If you look at table 3 and figure 1 directly floats and the argument is under ethnographic research is, you do the hierarchically table and the figure is just that table as a representative heuristic.
PETTIT: I think table 3 is fine, I think it sets it out well, one of the things I was going to say, when physicists talk about Einstein's theory of relativity equals MC^2 and that, they talk about an elegant formula. We don't have that type of terminology, before people start designing, before they even look at what they are going to pick or what they are going to do for a space, they should have in their mind set as the greatest criteria is what is the utility of this, is it fit for the purpose, is it going to be aesthetics of it, quality of life, your framework that everything else sits into.
MC: If you look at table 3 the hierarchical table where would you see utility in that, your concept of utility fits into the table diagram?
PETTIT: I would think it would have to sit under law.
MC: Do you think it would sit under law as opposed to looking at utility, some people call it characterisation, in the pilot study they said characterisation in the Australian language doesn't fully capture content and they wanted facility contextualisation and stuff like that, do you think utility would sit more with infrastructure?
PETTIT: No I would be putting it below law and quality of life, aesthetics, efficacy, all that would sit under law.
MC: So would it before contextualisation or would it be under contextualisation?
PETTIT: Where is contextualisation?
MC: If you look at security you've got law and then you've got facility contextualisation.
PETTIT: Yes between law and facility contextualisation. I think they are the fundamental planning principles that when you are selecting products they are the sort of things that you have got to have in mind.
MC: What about your efficacy or your fit for purpose, where do you think you would have that in the table?
PETTIT: Again, I would have it as a planning principle.

MC: So probably planning and design, so down with planning and design, underneath that between security theories and principles, you would have fit for purpose.
PETTIT: Yes. It's one of these things, it's a bit like the risk management standard, where you go right through the risk management standard and go down to treatment, then you have business continuity management, which is only basically the same as the risk management standard.
MC: What about aesthetics then, where would you put aesthetics in relation to this organisational structure?
PETTIT: Again, it could be considered at both levels, just below law and above facility contextualisation and planning and design. I think a lot of it could go in both areas.
MC: That gives me something to put to the others as well at this stage. One of the things that came out of the pilot study focus groups, when I looked at the table and said what do we see, a key thing that came out that we have to keep the science that underpins in each of the knowledge categories some areas it would be psychology, some would be the science that comes out of physics such as detection and technology, maths and geometry, basic principles of reflection and retraction, the physical resistance to pressure, the barriers, so what came out of my focus group is that you have to keep the science that underpins the pursuit of each categories objective. So if you look at CCTV, basic principles of maths and geometry .....
PETTIT: Some of this stuff, I don't think there is any one place that it should be, it may fit in multiple places.
MC: And that is where the MDS comes into it, in terms of the hierarchical table this is what they call a qualitative analysis, when I do the structural strength, where structural strength comes out in the MDS, it's a mathematical relationship, if I have 100 people respond to the survey it is based on the mean of its location in relation to every other concept so what that map gives you is a statistical location in relation to how it is similar or it contrasts every other concept. Some of the concepts can go in a number of places in the hierarchical map, that's why I need to use the MDS map as a follow up because that then gives a different representation as a graphic.
PETTIT: A lot of this stuff will be provisional.
MC: This is just the first iteration, comes from the pilot study and is an iteration of this as this is not seen anywhere else.
PETTIT: Clearly people haven't thought of aesthetics all this sort of stuff, it's a bit like 1500 years ago they thought the world was flat and they thought the sun revolved around the earth now the earth revolves around the sun; they were talking about whether the universe was expanding now they are talking about it contracting. These are all provisional knowledge, at the time it was considered true but as we understanding things more we know that they are no longer true and the new truth comes out and this is what I think a lot of these sort of things is it is provisional. Today with the limited knowledge of the experts that you have we do have experts that have got limited knowledge they are not going to come up with this you beaut stuff yet.
MC: Interestingly enough when you go to the underlying theory, I don't know if you read the underlying theory stuff I sent over to you in chapter 1, when you read that it will tell you that the fit doesn't have to be perfect, it just has to be useful.
PETTIT: The other thing I just thought, another term that comes to find is environmental.
MC: Actually environment believe it or not it actually came up again, it was one of those areas or knowledge concepts that did come up a lot in the word count analysis but

it didn't come up enough because I had to draw a line somewhere.
PETTIT: When you talk about environmental with occupational health and safety, you talk about water running off and flowing over from a dam, tailing a dam off somewhere else, the release of chemicals. It's application or its relevance to security, you see the spray this foam and suddenly you can't move, or you've got those big fire hangers where you squirt in all the foam and you suppress the fire that way or you've got that smoke cloak where you have all that smoke come out and cloud the whole area so they can't see what to steal. What are the environmental impacts of those products? Is it something that we should be mindful of because there is a law now that deals with environmental impacts, how is this going to impact on the environment?
MC: I think when you say environmental, looking at table 3 the hierarchical knowledge table, you have environmental but where would you locate it?
PETTIT: To be honest I don't know.
MC: I would put it between infrastructure and security surveys on the left hand side there. What do you think about that? Give that some thought because environmental is a big influence and if you look at how we establish the footings of a fence, we need to know the soil compact. If you are putting in deception technology in the ground, we put different technology in the ground for clay or sandy soil.
PETTIT: Take for instance fire detectors, they have got a radioactive isotope in them, now you collect enough of them you can make yourself a bomb with it. There is also the aspect as well it is encased in its metal container, it is not a health risk. I'm quite sure that at one stage they were using asbestos in safes for fire rating.
MC: they were for the fire retardant. When you talk about environment, basically that goes in two directions, you looking at environmental conditions and other more environment factors.
PETTIT: Environmental law, chemicals in the environment.
MC: And I guess that would be consumed, if you look at the concept of super ordinate, subordinate, environmental law would be consumed within law itself.
PETTIT: It could be but it is just one of those things that is out there, we know it's out there but no one has thought about where it fits.
MC: This is one of the problems, how do you teach this to a novice? If I'm teaching physical security, how I know that I need to teach you this and how does it fit together. How does the student know okay I see why I'm learning that, a good example is electrical power, why am I learning electrical power, why am I learning the basic principles of electrical power, now electrical power didn't come up as salient in this, when I did the pilot study I only used three texts and electrical power came up as a salient issue. When I did it across the 15 text it got dropped down but it was something that was carried forward and certainly a lot of the experts in the pilot study said you need to understand what power you need to draw.
PETTIT: Magnetic electronic waves and microwaves and all that, is there a health impact here with that. We say there is not but we might find
MC: There are a number of different articles on the effect of microwave transmission systems on people, when you test them you have to walk through the microwave zone.
PETTIT: So there are aspects here that are latent and are present but we don't understand them yet, not yet apparent. I think you've got to have a category of things that are present but not yet apparent how they fit, where they fit.
MC: That is where MDS will come in, what will happen, every item on the MDS map is related to every other item mathematically and so what happens is as a group summation the group cumulatively locates it for you because some things you can't put

in a digital map, it is a qualitative map, it is a deductive analysis map, some things aren't necessarily, you are not sure they can be in a number of different areas and the idea of an MDS map is that based on ratings with every other concept this is where it fits. That is why I'm using that for my next phase of the study. What I'll do is I'll take these concepts and reduce them down to maybe 40 and then put them into a questionnaire but I'll split the questionnaire into three and as each person logs in and does it they'll do a third of the questionnaire and then by the end what we will actually have is a mathematical map of where the concepts are related to each other. The only problem with that is, it is not as easy to understand as the qualitative maps so you need both maps and one will help you interpret the other.

PETTIT: This table 3 if you had heat maps which would show security as your big circle and then little dots of different size as to its relevance in that domain.

MC: In the pilot and this study, when I've put the tables together to make table 2 I also had a word cloud that was calculated by Envivo so I can send you that. What it does was the most salient terms appeared bigger and in bolder text and as the terms dropped off in their occurrence across the texts they become smaller and it does the same, it takes probably the top 100 terms and arranges them as a word cloud, so I can send you that to have a look at. What was interesting when I did my table calculations when I compared it to the word cloud, the two were congruent.

PETTIT: It would seem to me that some of these will mass together, certain terms will mass together.

MC: And you see that in the word cloud. So what do you think are the three most important knowledge concepts of physical security?

PETTIT: I think you have got to understand context, because context fits into things like quality of life, your aesthetics, utility, it all sort of brings that all together.

MC: Also I guess the level of security.

PETTIT: That would be the next thing. You would have to understand the level.

MC: So under context what would you have, what's the second most important?

PETTIT: I would say understanding the level; I don't like the word level.

MC: It's a hard one to change though, level is the one that came out and in fact even the other experts admit, that is the art they talk about the science of security being understanding the physics, the technology they understanding the resistive in terms of metallurgy for barriers and things like that, the art comes back to setting the levels. If you look at what you do as an expert you are looking at was the level set reasonable.

PETTIT: I wish I had a better word for categorisation of the security need.

MC: It is a hard one and in the text they use levels. It's a hard word to replace, I found the same and that is why I left level in there because it is something that just keeps coming up, we talk about levels of security.

PETTIT: The last thing that I think that is important in physical security or in indeed any security is review. One of the problems is people treat security as set and forget.

MC: Do you think that review should be in analysis and evaluation.

PETTIT: It is but it is after the fact, it is revisiting a month or two years later. Next theft after the next theft later, we plan a factory, we do our security, we do it to two other factories, we assess the risk of who is going to steal the capabilities, the tools they will have available to them, so we design it. Two years later we broke into factory A, we go out and we have a look at it and say 'what happened here?', they came in through the back grill, the back window through the toilet'. Now our records show that when we built this factory we had grills put on this, where the grills went, they are not there.

MC: Are you talking about security decay there?
PETTIT: Yes, has something changed or, and then you go and talk to the manager of the site and the manager said oh yes we had an OHS inspection and we were told to take those grills off because it breached the fire code or something like that. Then I've got to think, if it breached it here I should go and check these other places. So off I go and have a look at the other sites and they have been removed too, I've got to go and think about my physical security again, do I put more sensors in, do I put a bigger fence up. So periodic review.
MC: Interestingly both in this phase of the study and the pilot phase the concept of analysis and evaluation was something that was constant, so you analyse, you evaluate the law in terms of understanding the legal content, you evaluate the vulnerability of the facility in relation to threat, you evaluate the infrastructure needs, you evaluate the security needs, you actually evaluate the system once it is conditioned. So would you have analysis, evaluation and review?
PETTIT: Yes, maybe. Because these things are not necessarily linear, review is not necessarily at the top of the list but that does not mean that it is not done at the end of the process. This is not a one, two, three, four and four is always the last number.
MC: In the focus group people talked about 'how do you really separate analysis and evaluation and are they one or the same'. One of the participants said you are splitting hairs because they are pretty much related. Would you go to perhaps a category of evaluation and review or analysis and review as opposed to analysis and evaluation?
PETTIT: No, you look at it evaluation you work out how, it is part of efficacy isn't it? Then you go back to relook at it.
MC: Maybe have review after report writing?
PETTIT: Could be. When Henry Ford first built his first car they didn't have keys in them, you started by pushing the starter, there was no such thing as car theft. Why would he have to design a car with a key, no one steals them, the only reason people didn't steal them was a) people didn't drive and b) they didn't have cars. Next minute he is having to put keys in them.
MC: So really review for you is another category again.
PETTIT: Yes. I really think you have got to look at how things change.
MC: So what would you call it, review, reviewing, reviews?
PETTIT: I think maybe security review, I don't know. Things come up for level – like proportionate, level of security, proportionate security risk, commensurate.
MC: Level really captures it doesn't it?
PETTIT: Yes, level is commensurate with the risk, it's part of the sentences it can't be replaced with one word. Let's look what it says review here, analysis or check inspection report, revision, reassessment, maybe reassessment because your risks change, one of the things is risks are dynamic.
MC: If you look at the way I've done the diagram say figure 1 and table 3, you see things like report writing covers everything from law down to ..... inclusive and analysis and evaluation covers everything from facility procedures up to ..... security that covers law as well. So you are analysing and evaluating every aspect of this it overlaps every single category.
PETTIT: Report writing is very important and the fact that when police investigate a crime they know the elements of the offence, so if someone steals your car the first thing they do is get a statement of you to say 'no I haven't given anyone permission or authority to use my vehicle'. Then all they need is a time, date and place it was taken. Offender's name, this jurisdiction, did use this vehicle, registration and so on without

the lawful authority or approval of the owner. So it is important when you write these reports that you know what the elements to put in there. This is what I find a lot of security people have got no idea of what the elements that they should be ticking off on in their reports. You see it at the security guard level, and they get there and they say something like ‘he was intoxicated and we used force to remove him’. Well there are aspects, where’s your assessment, how did he come to your attention, questions that you would be expected to be answering in the witness box you should be putting in those reports.

Appendix L

PHASE FOUR FOCUS GROUP TRANSCRIPT EXAMPLE

Focus group: Fraser, Peter, Brad, Garrhett, Clint, Nick, Brian and Michael Coole	
MC:	At the start of this what I sent out was a number of maps and tables of knowledge areas that either the text books or different people that have participated in the studies over the last two years have said this is the area, in order to get a clear focus for this, the focus that I've taken is only physical security, but when I'm looking at physical security a lot of people sees it as different. Some people see it as physical barriers and focus on the technology or some say operation security is different to what I do in terms of technology. What I've done is gone from the text definition so physical security is a system practice device of a tangible nature so even operational security that forms a procedural element of actual physical security and that is probably the best way to articulate it, so we do have technical, physical and procedural combined to produce an outcome, which is really the focus of this study. In terms of knowledge category areas there are a lot of staff that came across as core knowledge, other knowledge came across as more enablers to professional practice and so what I'm trying to understand is what is the knowledge that a graduate security person needs within the practice domain of physical security, or the skills sets. You will see with the maps that you have, the first one figure 1 is a qualitative map that I did and that came from a table you have as well - table 2. Table 2 comes out of ethnographic research where we look at a culture and look at how things are related to that culture hierarchically, the argument is that as things are related in local connections actually starts to give us, not only the content of a domain of interest but also how its connected, how it relates to other content in that domain. The other map you have, the more confusing one is that multidimensional statistical output that is based on the comparisons between these concepts from a sample of a survey questionnaire so it's a mathematical analysis of how these sit. What is interesting when we look at the two maps, the argument is the dimensions that the knowledge relates to is either diagnosing a security problem or treating a problem, where we have a less complex problem the diagnosis very quickly leads to treatment or in fact we can work backwards, where it is actually a very complex or new problem we go through that professional inference which is that core knowledge security theories etc. If we look at some of the clusters on the MDS map do correlate with the hierarchical structure which is very pleasing for me that it came out like that. So based on these maps and the table of knowledge the first thing I want to be looking at in terms of articulating all the formal knowledge systems, based on these maps as a group what do you see is the foundational knowledge unit requirements to be learnt by security professionals before they graduate as officers?
Nick:.	When you say graduate are you talking about a basic industry qualification or are you talking about a tertiary or....
MC:	The argument with professional literature which is quite interesting is, and it's

a bit confusing in security, the argument professional literatures says if you are truly a profession you graduate from a course that teachers the same knowledge and then you go out and develop later on so I'm looking at something that would graduate from university but that may not necessarily be an under graduate, for example – last semester I had an engineer who knew nothing about security, he was doing our post grad stuff to learn about security to become a security focussed engineer. So he is a novice in security even though he has an engineering qualification. So I'm looking at someone who knows nothing about security for them to go out as a graduate and be developed - what are the knowledge areas?

Garrhett: Once they come out of the degree, the outcome is that they can go into a variety of different security fields, so we are not basically talking about coming out and saying specifically you have to be a consulting, or coming out and saying you have to be a manage a guard force or be able to be a corporate security professional. Coming out of this degree should let them be able to do all of that, is that right?

MC: What I'm looking at Garrhett is only physical security so if you look at security management it has a different knowledge structure to someone who works for you, so I'm only looking at, in order to get some sort of bounding for this study, so someone who wants to go work in counter terrorism for the Federal Government, I'm not looking at that. I'm looking at someone who is going to go and diagnose security problems and help design and commission a system to mitigate that. That may be in aviation, stadium or casinos but the general thing is we have a security problem that is focused on the physical not necessarily counter terrorism or anything like that. So while a broader security degree may look at all that what I'm saying is what is the knowledge of just the physical specialist, consultant adviser.

Garrhett: I think looking at the core foundations I think every security professional needs to have an understanding of risk and I think to apply the physical security because they are going to have to still apply in the big picture and the linkages with the other departments. They are going to have to know the security concepts and theories, like defence in depth, crime prevention through environmental design, so I'm not saying this needs to be their major the units that they do when they leave but I think as the grounding when they first start this is like where they should be starting to get an understanding of this base.

MC: When you look at the map, one of the things that came out the other day is that the top section of this map actually sits more at that diagnosis, the yellow section sits at the reasoning that profession inference, core security theories and a lot of the bottom part of the map is more attuned to the designing, the treatment solution knowledge, the engineering, the science knowledge etc. What you are saying is we look at the top of this map or we look at the knowledge clusters in the centre of this map and that is actually what we have got.

Garrhett: That's a good outcome.

Fraser: I always have a big, not a problem, it is very important for someone to have that grounding and understanding of risk but one of the things that I always see a lot of is someone with that and then no idea or little understanding of the technical side so it's great to do a risk assessment, but unless you understand how the systems work and know the practicalities of them, what the challenges are with then and installing and how they work and operate, if they don't understand that as well, how can someone say that they need to implement that as a mitigation strategy. For example a PDS on a prison, if you don't understand how the micro phonics and how they work them how can you say that is what they need. But I think as a first basis at least having an understanding and grasping of the concept of risk management and those other concepts and theories, you can learn some of the other stuff to a certain level but to be a professional looking at the technical side. So someone like Brad, I understand technical stuff but I don't know anywhere near as much as he does, particularly if you look at x-ray machines and baggage handling systems, yes I understand how they work, I know how they work, I could design a system but I've got no clue compared to what Brad has or understanding of that, so I think you have to look at the different levels but if someone is coming out as a junior then they can learn some of those concepts but they have got to have that foundation principles.

MC: And that is one of the things we look at and one of the other questions is what is the line in the sand, I had a chat to Brad about it the other day, one of the reasons why Brad is here is that he is probably one of the most knowledgeable people in the country in terms of that deeper technical stuff but not everyone is going to be like Brad, so what is the line in the sand and one of the questions I'll look at later on is what do we need to learn as a person starting as a novice and what is best left post grad to the professional development later on, so it might be the higher technical aspects, what does the group think? Based on the depth of experience in this room, how do we draw the lines in the sand? So what you are saying is they need that fundamental knowledge of all of it.

Fraser: Yes, I think so, I think a shallow broad brush is probably a good start, but I think when you look at, you need the ability to start from first principles and look at it from the top down and I agree with Garrhett that every piece of technology we implement or every building change or architecture or planning or any of it is built to mitigate risk. First of all you need to understand the risks you are mitigating then if you look at it from the complete other end of the spectrum all you are looking at is the laws of physics. You don't actually really need to know as a security professional how micro phonic cable works, what you need to know is that you need to detect vibration on that fence if someone is trying to climb it or put a ladder on it or however they are going to breach it, so that you can go then and, this is where you have to admit that you don't know what you don't know, and go and seek out a security technology professional and say I need to detect movement or sound on this barrier, how do I do it? They go here are the products this is how they work, whilst I understand and I would love to see all security consultants have a very very good foundation in how the technology actually works I think it is more

important that they have the knowledge of what is possible and what is not and how to apply it and they can go to someone else to get the information on how it works. Because a lot of the guys that understand the technology in detail can't look at from the top down and therefore they don't get the risk that they are trying to mitigate.

Garrhett: I find that a lot as well, not only in the team I have but in all areas of security when I am going to a client or when I was working in the UK. Security is a merger of these corporate operational managerial procedures and technology and I think as a foundation there is almost two different personality types who prefer one or the other. So you've got people who just like technology and come from a technical side and you've got people who prefer report writing and writing frameworks and management procedures and it is not just in security, it is almost like a different personality or trait of the individual and trying to merge them together in to one person, it is very difficult to find someone to hire who has both those skills in their personality who is willing to do that, in our team we basically will hire technical people and we'll hire report writers and put them into the same team because they need to bounce off each other's skills. I saw that in Home Office as well, we actually had technical officers and science officers and management officers and it was the combination of all those skills together. It is difficult to find one person.

MC: What is the ultimate goal? One of the things I've had to come up with and a lot of people don't like the view that I've formed today, my view is that there is no such thing per say as a security professional in a group phenomena, we are all professionals in what we do, we are all professionals in the way we carry ourselves but if you compare us to law, law is a recognised profession and everyone who is going to work as a lawyer does a general law degree and then they go and they may specialise in copyright law or criminal law so there is sub division specialities within that, and within those sub-divisions specialities they all learn the same, on the job development is individualist to everyone of those people but they all learn the same general knowledge. Same with accounting, you go into accounting and some people are focussed on stocks and trades, which is different to someone who does your taxes for you, but they all came from the same basic knowledge structure and then they do their subspecialisations and professional development. I understand what you're saying, one of the things in the literature on professions is that profession is underpinned by the department of learning or science on which it is based. The argument is that professionals should have and that is question 3, it is argued that higher education students should learn the science or knowledge of which their future domain is built and we are looking at the depth and scope for that, so it is interesting that you say that because I think individuals will develop their own expertise later on. But what is the base line, at the moment the physical security professional, I see it on Linked in jobs advertised, what is it? So if we were to idealise what the knowledge would be for you team as a base line and then people can develop their own interest, what would that be?

Peter: You would have to be able to have a level of competence to engage in

conversation in a meeting, basically if you come out of this degree and whether you're a undergrad who has come straight from school, because you have to break those two categories up for a start, because there is an expectation that a school leaver who has gone into the degree comes out and they are seen as being like in a graduate program, so they do get a lot more allowances etc. as people don't expect them to be able to design a facility. If you are a mature age student, particularly if you have come from a background working in a security industry or other industry there is an expectation that when you speak, when you are sitting at the table they think, you are not a graduate you are actually somebody who is supposed to have input that is going to drive decision making etc. like that. So there is a different kind of pressure there for a start. I think one of the issues that you are going to have is when you try and identify what the base line of competence is etc. like that for people are is that you have got a lot of information that you are trying to actually deliver to a person or as Brad said, all you are going to be able to do is give a very high level overview, so somebody can undertake a conversation and know what you are talking about but then if they got challenged then they are going to actually get a grilling. If somebody from a technical background then challenge them further they are not going to be able to answer those questions.

MC: That may be though that deeper knowledge they learn post grad and one of the things came out with this knowledge map, when I look at think gee there is a lot of knowledge in that area just for physical, forget about security management, forget about context areas aviation or maritime, just for a physical security person there is actually a lot of knowledge, I mean I wish I had a map like this when I started studying because back in those days you were trying to fit it together in your own head and develop your own relations. One of the things that I aim to do is develop something that a student can say why am I learning project management, how does this fit in? So I guess what I'm saying if you look at the different categories what you're saying is that they need a very broad fundamental basis.

Peter: The issue is that you are calling them physical security professional but the reality is when you bring all these things together it becomes that definition of a security professional because if you applied CCTV and stuff like that, CCTV well you've got to understand its use for monitoring an area or confirming a breach or an alarm or something but it's also an intelligence gathering instrument. I think it is very hard, your definition of a physical security professional, it's good to separate from an IT or a cyber-security, I think people get confused quite often when they see those two, they go security professional and its someone who works in cyber.

MC: And this is the first attempt, I've tried to articulate jurisdictional boundary to be honest, because it's been hard to leave that out.

Peter: I think physical is a good term to do that because, I think what you've got to do is go away from traditional physical security which is everyone just thinks it's just barriers, locks and stuff like that so I think the use of the name is that is pretty much at the end of this degree that is what you would come out as, as a

physical security professional.

MC: One of the guys from AECOm said to me, CCTV has its own body of knowledge, risk has its own body of knowledge and so what you see, it's like Brad if you look at detection sensors, it's an existing body of knowledge, electrical theory has its own body of knowledge, so when I started putting this together I realised there is still a lot of knowledge areas with their own body of knowledge so what do we want our graduates from a program like this to come out with, and at what level?

Fraser: I think you said something good before, look at legal professional, medical, engineering, law – they all have a based on what you do, so you become an electrical engineer, you can either go into building services and work on Bunnings and stuff or you can do real electrical engineering and do HV stuff, work on power stations, generation plans but you still done the same basis, same with legal, same with medical, and you specialise and realistically I think that is what you are getting at, there needs to be a level of what we can do with security and then move into different areas.

Peter: but how do you do that Fraser, one of the things is you identified there an electrical engineer, so they all do their base line theory but then they go and specialise because there is courses etc. to deliver that, there isn't courses to deliver.

MC: Not yet because we have not asked for them. Nick you teach security now, what is your focus?

Nick: Risk, risk risk risk because that's where we identify what we have to treat, risk assessment and part of it is consultation and mitigation, so I'm talking to people like you saying I want to do this how can I do it. So for me risk is the most essential thing and I'm not talking a basic level of risk I'm talking about risk where you produce a report based upon tangible evidence to tell me what is going on or what could go wrong or whatever and how can we treat it. To me that is the number one thing I am looking for. They have got to be able to walk into a room, sit down at a table and say here is my risk assessment, here is my treatment, otherwise what else are we doing.

Peter: One of the things though when you talk about the risk treatment is that very thing is that unless you understand what each of these elements is in the physical security environment you can't do efficient treatments because you don't know whether that treatment is going to be in line with what the threat is, so it's got to balance the threat with what you would treat it with.

Nick: Part of a risk assessment is communication consultation and that is why I get people to identify the stake holders I need, I say come on help me with the risk, this is what I'm thinking, what can you, so I don't need to be an expert in that, I should have some background knowledge as you said, I understand that domestic alarm system is not good enough for warehouse, I should understand that I can get .... radar, I can go for access control, I can go for, I need to get

your input to say this is going to cost 1 billion dollar, 1 million dollars, 100,000 dollars.

MC: You are still drawing on, you say like a domestic alarm isn't good enough for a warehouse, so you are still drawing on core technical knowledge to make that analysis. For instance a lot of diplomas in security risk management where a lot of people go and enrol in them and do them, but when you actually look at what they teach, most of it is risk based or a bit of safety or a bit of this but there is no core theories of security.

Nick: That's because you haven't done .....

MC: To be honest what this is about is saying what does a graduate need to do, if you go and do, TAFE is still a post graduate from high school environment, if I was to do a security diploma I would expect to come out with some security core knowledge not just risk.

Nick: We cover risk, we cover in CPTED, we do units on security operations, the problem is the diploma we give now a days, if you did a diploma of security its equivalent to a diploma of management. It has 12 units, 8 units are business units, 4 units are security and we argue this all the time, for security diploma it must have security and they say oh no, our colleagues we deliver business units it's easier for us to deliver business units, what is the point of doing a diploma if you don't offer

MC: Part of my study when I say I'm fusing all this, the reality all this knowledge exits, I'm fusing it together from text books and experts, but the reality is what can we draw on, to show the evidence to say we need this much core security knowledge and we need to cover this and that. Question 3 if you see it here, look at the scope and the depth which is what we are talking about now, if we look at these maps, we are covering off on risk, diagnosis aspect, in terms of understanding the security plan and design, those core theories we have that professional inference and if you look at the bottom we have the technical stuff, technology, physical barriers, what is the core knowledge they need to come out with so their core knowledge might relate to diagnosing the risk, it may relate to understanding the core theory of security, the core principles of delay, the core principles of response and at what level, where do we draw a line and say this is professional development?

?Brad?: I think it is hard as well, what you are saying, security risk isn't like engineering risk or other risks where it is tangible, you've got all your stats, we are looking at qualitative risk assessments most of the time. One of the biggest things I've found and teaching CIP, you have all the students who are third year students who have supposedly done electronic security, risk and they come in and they still don't always have an understanding or a grasp of those foundation principles of those things. You sit there and talk about how a lock works and one of the students will go - hey we did that in physical security don't you remember that – No! A lot of it comes back to their personalities. I've employed probably a dozen grads from the degree at SKM, GHD and

Worsleys all combined, the good thing about teaching is you can find the decent ones and go, hmmm I'll give you a job or I'll give you a job. It may not mean that they actually have a deeper understanding or a broader knowledge base of security but they might have the personality traits that you may need to be a consultant. I think there is a bit of a balance act between the two.

Brian Tisdale joined the group and provided details about his background. MC updated Brian on the progression of the meeting.

MC: so we are focussing now on what is the core knowledge and a good example is say Garrhett, if you get a graduate tomorrow in your section, what is it and think about also the number of people here that have graduated from the course, think about the knowledge if you thought, I wish I covered this when I studied. What from someone who is a graduate from your program but also what is the stuff that people think I wish I got taught this before I ended up here?

Garrhett: For me going into consulting it was the management of the design, going in and not understanding the phases that you have to go through to get to the end product or the master planning, concepts, schematic detail design, I didn't have an understanding of that process and how to interact with the clients and what information they needed and what the other disciplines needed at the different stages to develop and get the final product so I think that was what I came into consulting and going oh wow this is what I actually do, which is manage designs, not just design something once, I have to manage the process from the start to finish and that was the biggest eye opener for me going into consulting. I don't know if you guys have had a similar experience?

MC: None of that came is covered in any of the text books Garrhett, that is one of the problems, that came out a lot in my in depth interviews that I did, that was a theme that kept coming up and recurring, how you go from the initial idea to a detailed process to actually commissioning and testing and end product.

Peter: But that is no different to any other engineering discipline when you look at it from that perspective, whether you are consulting on security or whether you are the electrical consultant, the lighting or the environmental consultant, the process is exactly the same, so whilst I think you could probably cover that off in a unit I think that is probably something that needs to come from a general engineering degree because that knowledge base is already developed.

Fraser: I think is where things like minors and electives come in, is how you actually guide students to pick the right units.

MC: But this is what I'm saying, for someone to understand what to pick, what is the knowledge you want them to have, for instance if I wanted to come and work in your design team theoretically why would I go and do a minor in business necessarily if I had focus on engineering skills initially.

Fraser: One of the biggest things would be if you are consulting, contract management,

and understanding of that because that is one of those things that when you are talking about managing clients, if you look at organisational behavioural type stuff going through it myself is people will come up with this what we want they document it, everything goes out, you put it out to tender, oh they change their mind and they don't understand that every time you change something it costs money, its extension of time, variation costs etc. like that, so if you have an understanding of how people think and that is what I think these minors and electives steering people towards the right ones, is that will give you that ability to actually develop so I think where you are saying Michael you lead with a core body of knowledge and then where you go off and you'll specialise but I think a lot of the things can be delivered at the uni, there is an emphasis on the student to work out what they want to do and quite often they won't have a clue what they want to do at the end of it because someone might want to go and do OSH as part of it because as we see there is a lot of this combining of HSSE and stuff like that so it's going to be hard to design the perfect course for what people want to do.

MC: I am only focussing on an ideal curriculum, so if someone said to me what is the ideal curriculum for a physical security professional in the future, because it doesn't exist now as it is anyway, what are the core units, what do we have to cover.

Garrhett: I think you have to cover both, if I can make it basic, the English and the maths you have to cover both of those and previously when you come out of high school and you think what do I want to do, do I want to do an English or maths degree, what am I strong points, and now with these contemporary science degrees, there seems to be an amalgamation of these two and you see that in sport science where you have got guys who want to do sports and can write the reports but now they are doing biomechanics and have to do all the maths side and I can see this in the security science program as well and the touching point could be risk but the foundation is, you have English units where you are writing essays and business cases and you've got your maths units where you need to learn the technical side and like you said before about getting definitions, I think we need to give the students a basis in both these fields just so they can communicate with each other, not necessarily specialise in either one at this stage but know the terminology, know the principles of each side so when you're talking to a contractor you can talk about the technology side, or if you are a technology specialist when you are talking to a client or a consultant or an organisational manager you know what his drives are and what his goals are, so it's about defining both the maths and the English side so they can communicate.

MC: So with that, when you say the maths and English sides, one of the things with all degrees now is they are very focussed, focussed towards the outcome of the degree so to the goal or profession. What I've tried to do with this map is that one had to go through concept reduction so I couldn't put all 98 concepts that sit in this map in this questionnaire because I would have one single ..... survey including my own. So what I had to do was reduce it to the hierarchical theme so when you talk about the maths or the English and I look at this I think

okay someone needs to understand threat so Fraser says talk about the threat it always goes back to the threat and risk so if someone needs to understand what threat means I do the goal of security or we look at detection came up as a salient knowledge area if we look at things like response or delay and barriers, these came up as salient knowledge categories, so I guess what I'm saying is should we be teaching, do they guide the knowledge categories that we want and then we teach the maths or science or English around those?

Fraser: I think it is important to have that definition of understanding upfront, like you said threat means different things to different people, depending on their background experience, so many variables in it but if there was a defined definition, okay this is what it is for a security professional and then you could move forward form there I think. But because it is kind of very subjective it's difficult to actually pinpoint something, saying this is the foundation principle we have to start from and then teach the principles and guidelines and everything else around it, until that is nutted out and defined I think it is very difficult to say.

Nick: But doesn't it come down to, don't you need the maths and English before you can do a subject.

MC: The trade-off is that the variation of high school leavers is phenomenal these days as an educator, it's hard, some students I get are really good, they could be engineering students and others there is no way they will pass high school maths. When I look at, a good example here is going off what Fraser is saying, if I look at the higher level concept, if you look at treatment in figure 2 and we look at the notion of movement and control, so you achieve movement and control with barriers and a sub part of barriers is delay so what we are looking at there is a broader aspects of the goal so we need to control movement, we need delay movement and we do that with barriers. Once we understand the role of barriers as you said in your interview, comes down to the mathematics of the delay, so what is the physical resistance of that barrier to the threat. So we are looking at a vehicle barrier to delay the progress forward so I guess what appears to be coming out for me is that we need to teach the goals, so we are talking about movement, control and delay and the maths that sits under that is that we don't need to be the engineer we need to know to go to the engineer for the structural resistance and understand what he is telling us, same as detection, if we look at detection and sensors as a knowledge area is an area within itself, we need to understand what we need to detect so what are the threats that pose a risk, I need to detect personnel, or contraband material which is contained in metal, and then we need to understand in theory how the basic principles of the technology work.

Garrhett: Or what its limitations are.

MC: Yes what its limitations, there is a mathematical equation behind the probability detection for a sensor technology, if that makes sense. So what I'm trying to tease out so what do you think in terms of these two maps, these broader knowledge areas and the depths and scope of that.

Fraser: I think one of the things you need to do is prioritise this. To me I would look at it if you were looking at security I think the way that you are explaining it there and this discussion is going, you would need to put systems theory up very high on your criteria, because that will give you context, when you start looking at, coz as you are explaining there I look at this and then I say okay I need to go and talk to this technical professional on this area and then I have to consider if you are looking at it from a, if we use the terminology of an English perspective so that quantitative qualitative way of looking at risk so I think that needs to be one of the things that you need to have a top down approach to this because I think it will be a lot easier than the way it is actually formatted here, it is sort of a bit disjointed in some ways when you are trying to say what are the key elements that need to go in this. I think an easy exercise would be to just prioritise and break down because that will actually help you identify what those needs are for a security professional at the end of a degree.

MC: And that is one of the problems when you look at develop this and also these other maps, it is hard to capture, one person will say this needs to be there and then another will say this is more of enabling knowledge base so systems theories applies to biomedical science and applies to pretty much everything, where do we actually organise. An example is one of my first iterations to this map CPTED was located back here with surveillance and access control and it was Kerran who said no it is a planning thing, yes it's a treatment outcome but it's a planning and design element, it needs to sit with that, yes it provides access control, it provides a degree of surveillance but it is still a planning and design. That is when you look at this, part of the problem is some of the knowledge structure won't sit right, some things are diagnose and treatment in the way that you interpret them, some things are, it is not necessary that clear separation so it doesn't matter to a degree as long as we know we need to teach systems theory, that is the first thing.

Fraser: Which is probably one of those foundation units, I think if you taught systems theory like the structure of the degree you come into it and 101 is systems theory, it will help for all these other things to actually fall into place and be more readily understood by students, particularly those that don't have the background that they are coming from.

Nick: ..... systems theory is there a big .....

MC: It has its own body of knowledge, but I've taught the principles in a week.

Fraser: You can simplify, you can break it down.

MC: As a unit, one of the first

Fraser: I think you are going to have to combine a lot of these anyway.

MC: That's right, a lot of these will overlap, but in physical security when I teach it, in the first week is systems theory, this is a system, this is the systems theory

defined, it comes from this basis of systems science and developed by .....and then you start getting them to put it together.

Fraser: Then you can go into context because you can then apply it to the context of systems theory how it applies to a physical security professional so then you have given that broader view of what systems theory is and then you can break it down and start guiding the students.

MC: It comes back to the next question, how should the learning units be organised. So we look at the broader aspects, we have diagnosis, the professional reasoning in terms of security theories and the more engineering knowledge that we have that achieves the treatment outcomes, how should the course be structure if you look at individuals learning units such as threat, as delay, as response, how should we structure that so that it makes sense that it follows that system it keeps talking about.

Fraser: I guess that is one of those things when you look at something that has a heavy maths or science focus, it might be something that you deliver at a later stage ain the degrees, because you build the degree to building their knowledge base and confidence so they can apply that maths or science to it so that might be one of those ways to do it and then it allows them to identify their weaknesses so when someone comes and have a nature affiliation to English but they want to do this degree they learn pretty quick they are all pretty much writing whether it be an essay or other, even that – I don't think essays are the right way to deliver these things because no one has ever asked me to write them an essay on anything, it is all report writing etc. like that. So I think that then you need to offer guidance to them as to, if someone needs to pick up their knowledge in maths or in a science you can guide them to do that as none of this stuff will be able to be all delivered in this degree because it is so specialised. I think you need to guide them, if they need to learn about maths or something like that they need to go and do their own additional studies.

MC: What needs to be learnt, what is the priority for learning units before graduation and what is it that you are happy to develop someone in. If all of you were asked to employ a graduate today and you wanted to employ them as a consultant, you employ them knowing you need to develop them. What do you want them to have now at this time in their life and then what are you willing to get them and yourself to push.

Brad: Three things - a very high level and basic understanding of risk; common sense; and the ability to use critical and logical reasoning. If you have those three you can learn or teach them or teach them to teach themselves anything else that is on that piece of paper.

NicK: ..... common sense

Brad: I'm not entirely sure, we have always said and Kerran says it a lot more bluntly than I do but if our clients found out that 95% of what we do is common sense we would be out of a job tomorrow but they don't.

MC: When you say look at the map and they can teach themselves, one of the outcomes or objectives of this study was to develop these maps so that someone can go look I don't know that so now I need to know that I need to know that. When a novice looks at any course they are going to do we assume a depth of knowledge but in actual fact they have none. They don't know that they need to know risk, they don't know why they are doing engineering mathematics for delay or for pd, if you get a student to sit there and calculate the probability of detection based on the statistical output of trials and errors they are going why do I need to know this, the objective was to produce a heuristic or knowledge map that allows them to locate. So they might not be experts in technology, in fact that could be their weak spot but they know it's their weak spot and they know how it fits in with other things and maybe that is something they can attune themselves to later on. A good example is a lot of people think because they read families of physical security they know locks, Brian will tell you there is a whole body of knowledge, I would never say to someone ill design a locking system for your facility, I'll engage someone like Brian because that is what he does, it's such a specialised field but how do you know that it is a specialised field.

Fraser: One of the things I think we are missing the point as well, we seem to be getting away from the foundation principles that students need to learn, and I think that also comes back to the industries we are working in, like I said before, if I'm looking for a student, a long time ago I'd go this is the student I want, they need to be able to speak to clients, they have got to have some communication skills, be able to manage processes, project management, especially from an engineering design process and I try and find a student like that and they were good. And then coming back to what Brad said, I went okay well, what can I teach them, so what do they need to be able to do and one of those things was be able to communicate because especially within an engineering function or general business, you have got people who are propeller heads, fantastic at sitting behind a desk designing the voltage drop between this and this or whatever, but put them in front of a client and if they want to be a consultant they are clueless. Not a smart person or anything like that it's just out of their comfort zone. Conversely if I go and sit down with brad in a meeting, even some of my meetings at the moment half of it goes over my head, but I can put the old tap dancing shoes on get up and communicate and find out what I need to know. That is I think if a student has the ability to do that all the other stuff can be taught so that they can get that through experience.

Garrhett: So maybe the best way to look at these is to say we have three students in front of us, they all have great communication skills, common sense, these other trait foundations, what separates them, who we are going to pick because they have got more knowledge in something in front of us.

Brad: I'd look more at their personality.

Fraser: I'd look at the one who is not afraid to say look I don't know the answer to that

can I get back to you tomorrow.

MC: Sure but what is the desirable knowledge you want them to have?

Garrhett: These are all sort of good attributes.

MC: We often talk about post graduate attributes, but they actually are a sound foundation for selection but consider that you have three people that have all these attributes and they score high what is the desirable, what would separate them in terms of the core knowledge that you would take one over the other. One of the guys earlier in my study said he actually hired a security graduate following a terrorism program and he said he very quickly learnt the guy could communicate but he didn't know anything about technical security which for him, he was in a design consultant engineering firm.

Brad: That was his fault he employed the wrong person

MC: He agreed, one of the things he made comment in the last focus group was the learning units need to relate to the objectives of the domain, what do we do. So he is designing physical security.

Fraser: That is where you contacts come into it because everyone at this table would say a different thing. Particularly if you are doing consulting work because it just depends, if you are building a prison as opposed to you're doing work on a piece of critical infrastructure it is going to be different the attributes that you want at that time.

MC: The common theme is a risk approach, the common theme is that we need detection, we need delay, we need response.

Fraser: Yes but you are going to emphasis different things, again you won't incorporate everything in there, you won't.

MC: So what do you need to incorporate as core fundamentals?

Peter: Is it possible to combine similar units together?

MC: Yes, absolutely. So what is the core fundamentals, so you may not learn everything about detection technology that Brad knows but do you need to know the basic principles of detection and how we achieve it.

Brad: If you break it down like that it might be better. As you said we've got risk, there's detection, and then so looking at the concepts of security, I mean we already teach CPTED, DRD all those type of things.

MC: So you think they need to learn that?

Brad: Yes.

MC: That is what I'm saying, what is the desirable knowledge that someone you've got has as a fundamental.

Brad: As a broad brush I think it is important to understand all those theories, principles whatever you want to call them, because then you can specialise in certain areas once you have got that foundation.

MC: So looking at the map, what do you think is core that a person needs to understand CPTED, defence in depth, detection, response, you don't necessarily have to understand the legal formalities of response that someone with 10 years in the police force does.

Brad: They at least need to know about it.

MC: Yes, and that is what I'm saying or Garrhett is saying, what is the desirable have this knowledge, what is the knowledge you want these people the core overarching knowledge.

Nick: If you go back to risk the management framework ISO2000??, context it goes to identification..... for example context is looking at ..... structure a course, you might do a pre-emptive course then phase 1 is we look at context, how the context affect security.

MC: that is as that comes as well and a lot of that will overlap.

Nick: Then the context with most that stuff will then is looking at the most important organisation what is key there, what isn't key, for example a gas burn, pots mean nothing it's the sulphur removers it's the cooling systems that mean everything.

Brad: Depends on who you talk to, pots can mean the lot

Fraser: If you go to Kwinana those little pipes that aren't detected, if you take one of those pipes out you can shut down operations for up to 3 to 6 months.

Brad: To determine what is critical and what is not. It's not always the big shiny things.

Nick: The stuff I learnt was actually Middle East stuff and it was .....

Fraser: But that is the different there is so I'll use that as an example say like Kwinana, it is for shared synergies between industries, it is the most intensified in the world, they are inter-dependent on each other and those little things that aren't protected, I'll tell you if you take one out, because it has happened where something nearly got taken out by accident, and that was three to six months it would have shut down.

Nick: Me walking in not knowing that I'd say do you have pots let's do this, you walk in saying hang on a second, and to me that is context you have got to

learn how to talk to people and understand what you are protecting and what you want protected. Then you move down to risk identification what risk do we have, Australia is different to Middle East, different to England is different to .. all this feel causes problems so that comes to identification and risk, things that happen to us reasonably in our area. Then treatments are things like your CPTED, situation crime prevention, defence in depth, that is how I see it anyway. Treatments are offered to the electronics security, physical security, going through all that stuff come to treatments, risk acceptance then its project management, we've got a piece of paper, how do I not take a bit of paper and actually take the words off the paper and put it into place, that is how I see the structure.

MC: And you think the structure of the curriculum should be based on that framework?

Nick: That is what I'd like to see someone walk out of a course with, knowing how to apply that and how to apply that in everyday use to a high level that is the goal. It seems to my mind that that actually builds upon it.

Brad: I think that is one of the biggest things and dare I say it, this is no disrespect to you Mick, academics and Dave said this when he worked for me, I reckon that every person in academia needs to go back in the industry to work between every 3 to 5 years. He would sit there and it was great, I'd get the red pen out and go to town on the reports and anything else he was writing because it was completely different way of doing things and maybe why I'm such a pain as a lecturer because I look at things from a client point of view as what do I expect to see which is different to what academia may teach. That was certainly the case when I was doing the degree, there were probably maybe one or two people that actually had any real life understanding the rest were pure academics. Trying to get that together and I think that is what you are saying, you have got to be able to understand go through that context.

I've just written a few things down here which is pretty much what we've already spoken about. Some of those foundation principles could be things like - systems theory, security concepts and practices, electronic security, security risk management, infrastructure protection, project management. I mean I know the degree used to have a PM function, I use that term loosely, but I don't know what it is like now but infrastructure protection as well breaking that away from CI because something may not be classified CI by the government but it is important to that client in their operation so it is still critical to them even though it is not classified as CI. So just breaking that down to infrastructure projection in general because that brings all of those things in together. I know my students, we go through risks, we go through- first assignment is a pragmatic and systematic approach required for CIP and they all sit there and go I don't know how to write this, do this or do that, so that is why you are here to learn. So trying to bring all of those concepts together, I think that is what you are trying to get at – what do we have to have so that they come out with all of that understanding of those things, which we know when it is so important to understand electronic security, security

concept side, CPTED, defence in depth all of those things, it's imperative to understand risks, its important they can communicate, they have a project management understanding, and regardless whether they are going to consulting or they are go into technical area of expertise or anywhere else they still have got to be able to plan themselves in a logical manner in everything they do, regardless of what industry or what specialisation they go to.

Garrhett: Looking at the foundation knowledge I know we are trying to identify what it is but if I could take a different approach and maybe point out just for me what it isn't and that might mean maybe we can start there so from where I am, I've boxed out law and this one adversary criminology, now I know having an understanding of law and regulations is important but I wouldn't say on a daily basis that knowing how our legal system works and how to enact the law is something that I would even look at. Because there are so many laws and regulations just knowing that if I am going into the aviation industry or maritime industry, I can have a look at the maritime act and have a look at this and see how that affects me but actually knowing law or a law degree principles I don't use at all.

Fraser: Do you think on that one then what would be better about that is the ability to interpret legislation, policies etc. and so instead of specifying that law, because you do need to know that but you are right as specific laws.

Nick: ..... Law standards, you know Australian Standards.

MC: One of the limitations I guess and why I've had to approach this as well, extracting all this from text books, they were all subsets of law for instance how to interpret legislation, if you do a count analysis that didn't come up very often but law comes up 6000 times. So law becomes an overarching theme, cultural domain analysis cover term, but within that cover term we need to know what we need to teach in law. So what you are saying is correct, do we need to know how a bill is created.

Brad: That depends on where the student is from as well, which legal system is based on so if we have international students from the US, the middle east which we do they are all in complete different context.

MC: That is spot on that is actually good that you are able to say what don't we want.

Garrhett: The other one I've boxed out so far is adversary, so basically I need to know what my threats are but I don't need to know the criminology basis behind that, this is sort of like a crime prevention from a policing perspective or what motivates them in the geographic in which they are from, I am not going to be able to influence that they come from a poor family or they have got these other mental problems, I don't need to know any of that. So from my perspective understanding what makes up a threat, their motivation and everything, yes I need to know what makes it up but I don't need to know the in-depth of what my adversaries are. Does anyone else agree with that?

Brad: I think it is important that any student have a basic understanding that understanding the adversary can be important and it is not something they need to know about off the bat but I think from a knowledge perspective it really needs to be there because they need to be, there will be that time where they need to sit down and go I am treating a specific risk against a specific type of disaffected nut case and I need to understand exactly the risk I am treating because I need to be able to isolate that and not affect the rest of the population and so I think from that perspective you don't need to come out of the degree with that sort of knowledge but you need to come out of the degree with that little word in the back of your mind so that at some point when you actually have to sit down and say I've got to get into this persons head you need to know that.

Fraser: But that is probably going to get encompassed within if you are teaching about threat and under the risk banner etc. like that , that is going to inevitably come out, the concept of an adversary.

MC: Adversary is an American terminology as well, one of the limitations we had and we have it in a number of professional domains, this concept of ..... cultural language, language that means the same across different language and it doesn't, a lot of the text books on physical security that I had to do the initial extraction from, they are all American centric, so adversary is their term, some people in Australian don't like the use of adversary because there may be legal implications that they read into. A good example, I was asked to provide advice on security for a library and the best thing really was a CPTED approach and when I actually sat down and talked to the library manager she said to be honest the biggest issue I have is teenagers having sex in the library, that came out as their biggest threat, we have book theft and destruction covered but we are getting more and more teenagers in here after school unsupervised and so what they actually needed was a layout where the natural traffic patterns provide the perception of supervision.

Brad: Which is then using security principles for a non security event.

MC: So it is context but it also comes down to that broader thing of, the term adversary doesn't fit that scenario if that makes sense.

Garrhett: I think maybe what I'm trying to say, I don't need to know why people are committing the crime, I don't need to know the root causes, social implications and how we can treat that, I'm not interested in how society can treat that, obviously I am individually but as a consultant I'm not trying to change societies to help them.

MC: No, and that is important to have that dissection in criminology, some of the theories such as situational crime prevention gives us a framework to understand how we apply the engineering tools, but do I care about biological differences in people and how that leads to offending, as a security person I don't care, as a criminologist it was interesting.

Garrhett: I've also had a look at ergonomics and ergonomics is really important when I'm designing a control room or making someone comfortable but I wouldn't say that more than 10 minutes on it in a lecture is probably too much, a waste.

MC: It is something you need to know exists but you don't have to teach it in depth.

Fraser: Once again that is something that comes later, as a grad you don't need to know.

MC: That is the most important thing, what can come later, what do you want the graduate to have and what can come later?

Clint: I think you have to consider what does come later as well though, guys are coming out of the course and the post graduate learning isn't really there. Unless you get thrown into one of the graduate programs with the engineering firms the guys are coming out of the course knowing not a lot really, this is from the technology and industry side, in terms of networking and integration and that sort of that, so I'm more looking at the green section there, is that learning isn't there in industry unless you are jumping into where these guys are.

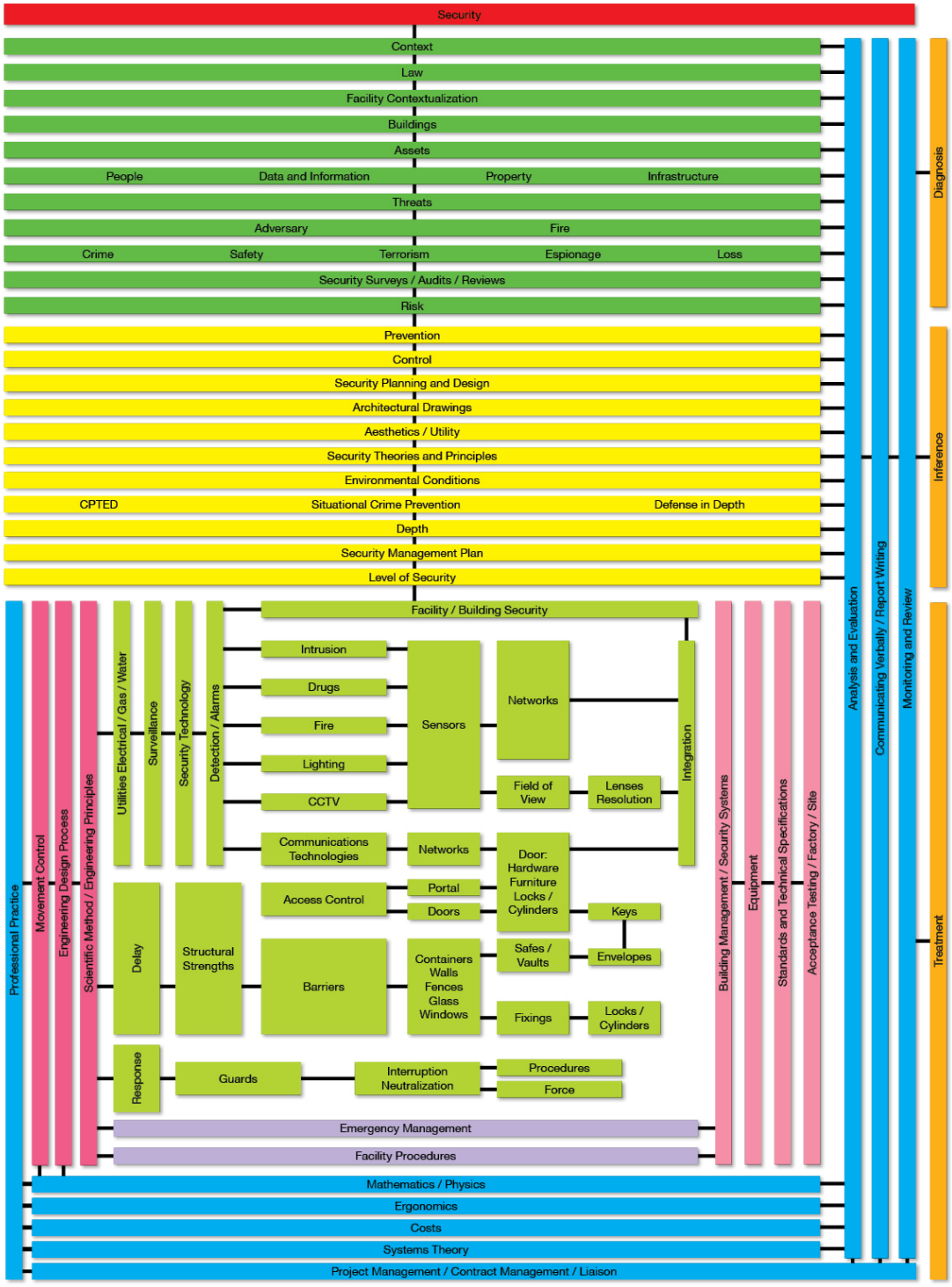
MC: That is one of the problems for us we can only teach to a certain degree, if you had the perfect course you would be here for seven years, which no one is going to spend 7 years studying, engineering's don't spend 7 years studying, they go into an engineering firm and that is one of the biggest issues coming out of security is medicine has a very clear pathway, you graduate, you become an intern, accountants get hired as junior accountants, lawyers carry books around for a year, security needs to understand exactly what you are saying, that learning must come, if someone gets picked up by Garrhett's team they are lucky, for the other 50 people what are they going to do, because there is only so much, I think Kerran actually said, he said he only has ever used less than 10% of what he has learnt in his engineering degree but you don't know what they 10% is. So any degree doesn't matter. Kerran's view is that any degree you do - you are going to use less than 10% of the whole degree in your professional context but you don't know what that 10% is.

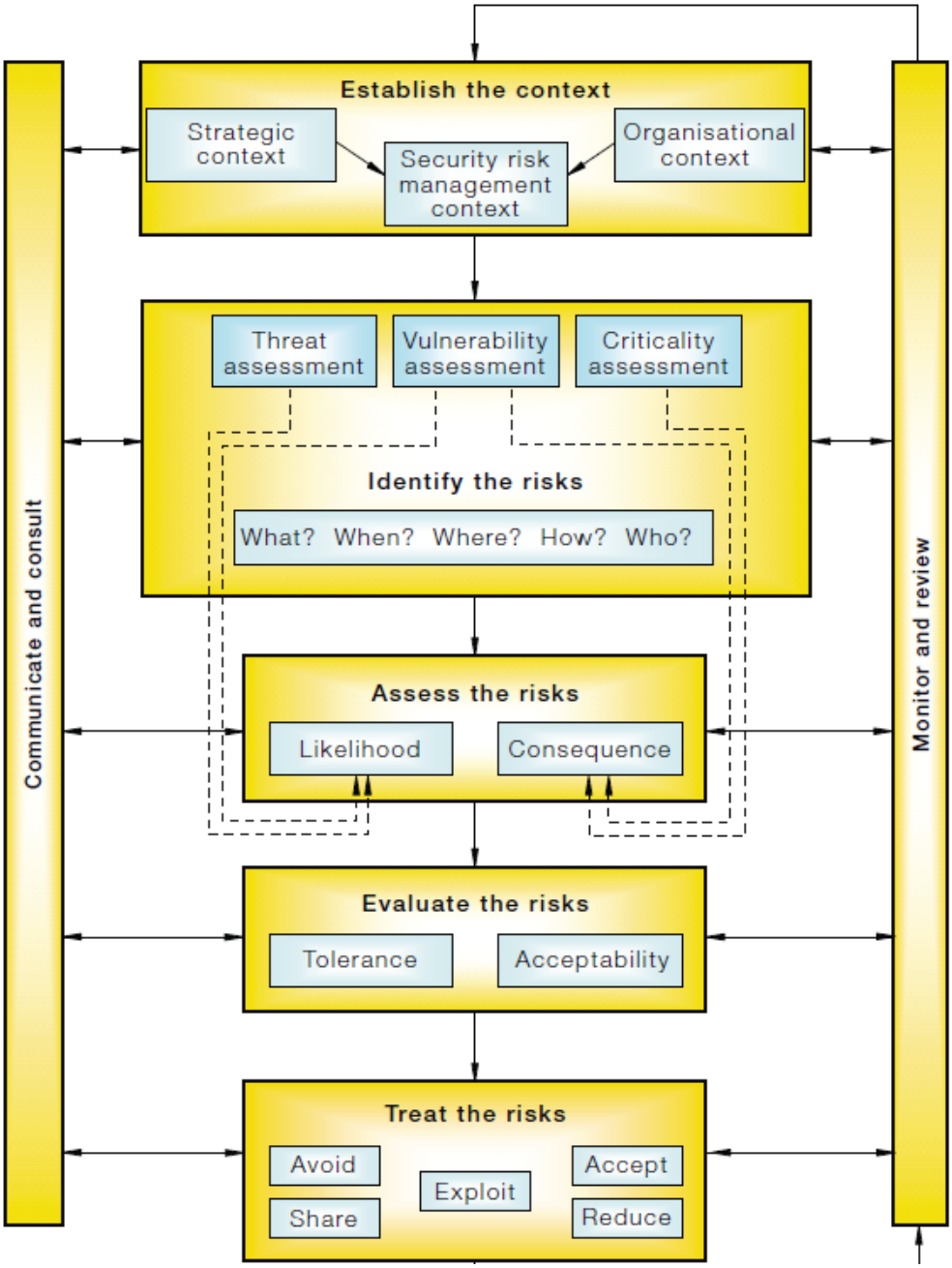
Brad: I think we are getting ahead a little bit there, if someone goes into a grad program its fantastic and having put a few people through that it is great for them, they do their four years in the grad program and they have all the stuff they need to go through, but for all intents and purposes they are employed by Jacobs or whoever as a graduate engineer, so on the books they are a grad engineer, they are not a security person or anything else they are a graduate engineer. I have seen time and time again there is individuals who work in the engineering side who are very very smart, know their stuff, so you've got guys designing process control systems or comes guys designing elementary networks, radio frequency for stuff which you would use for security as well. From a security point of view you would go you guys don't know what you are

doing, this is for security this isn't for that. They do know what they are doing they are just not licensed to do it. So I think a lot of the time there is an expectation that a grad will come out as an engineer and they will understand all these principles that they are supposed to but because we don't actually have like you were saying the same pathway, it is very difficult for them to be able to have anything definitive to say, this is what you need as you finish, which is hence this whole thing.

Appendix M

Risk Management Body of Knowledge Relationship




Establish the context
Strategic context
Security risk management context
Organisational context
Threat assessment
Vulnerability assessment
Criticality assessment
Identify the risks
What? When? Where? How? Who?
Assess the risks
Likelihood
Consequence
Evaluate the risks
Tolerance
Acceptability
Treat the risks
Avoid
Exploit
Accept
Share
Reduce
Communicate and consult
Monitor and review