School of Public Health

A Soft Approach to Management of Information Security

Helen Leslie Armstrong

This thesis is presented as part of the requirements for the award of the Degree of Doctor of Philosophy of the Curtin University of Technology

December 1999

ACKNOWLEDGEMENTS

This thesis is dedicated to my late husband, Peter Fillery. Peter contracted terminal cancer and died before the thesis was completed. Without his creativity, support and continued encouragement this doctorate would not have come to pass. Peter challenged my thought processes when I least wanted it and encouraged me to think laterally. You always wanted me to finish this work Peter - may you rest now it is complete.

Such a large piece of research cannot be completed without the aid of some very special people. Professor Ian Rouse and William Paul, my supervisors, took on an immense task in the latter stages of the doctorate and assisted in bringing all my work together into a coherent whole. Ian and Paul have given me much of their time as well as tremendous support. They have shared my experiences of frustration and achievement – thank you for your dedication and wisdom, and your belief in me. Katerina Andronis provided not only the site for the practical work involved in this research, but also continued encouragement and enthusiasm over the extended period of its undertaking. Katerina is a lady of action, and seemed to hold time in her hand whilst manifesting the physical resources needed for the research. Her enlightened management style should also be applauded.

I wish to thank my previous supervisors, Professor Lynda Harvey for her dedication, her powers of clarification and gift of synthesis; Professor Graham Pervan for his perseverance, support and advice, particularly through my time of personal turmoil; John Palmer for his advice and friendship; the late Dr Roger Coldwell for his enthusiasm and ideas, and Dr Nicholas Chantler for the many hours of in-depth discussion and his wisdom. My thanks also extend to Dr Mohammed Quaddas for his assistance in the early stages of my research.

My parents have shared my laughter and tears. I thank my family and friends for their patience and sympathy throughout the many years of my study. In particular, my son Greg provided encouragement even when he had to compete with the computer for quality time with me.

To my close friends, I only had to ask and you were there for me. A special thank you to Colin, Luther and Elestial – time stands still when we work together. Thank you from my heart and soul for your love and guidance.

This doctorate research has been beset by an enormous number of obstacles. To reach this stage of completion is nothing less than a miracle and I believe it must have been supported by a host of angels.

May God bless you all.

TABLE OF CONTENTS

1. INTRODUCTION

1.1 BACKGROUND TO THE RESEARCH

As technology has advanced over the past decade in particular, the security of corporate information has become an increasing concern to management. This concern has developed as the rate of computer-related crime has risen, particularly in the areas of fraud, theft, sabotage and hacking. Other more subtle influences upon the need for security have resulted from both changes in organisational structure and culture, as well as global social, economic and cultural changes.

Information security has undergone a revolution during the same time. Corporate office policies and procedures for the protection of sensitive information, which have evolved through painstaking trial and error over the last 200 years, have been 'reversed, obviated, or obliterated in less than a dozen years' (Weiss 1992b, p46).

Studies of computer crime and security management continually report that concurrent with this era of technological advancement there is poor implementation of security measures and a low level of awareness in general about security issues. Managers need to be well informed about the nature of risks in order for them to respond (Hains 1992a; UK Audit Commission 1994). This, and other research, shows that managers often fail to understand the risks inherent in the usage of computer technology. Executives and employees are not well informed regarding security issues and protective measures are generally implemented in a piecemeal fashion, often in response to security problems or violations. It appears people at all levels within organisations are not cognisant of potential exposure areas that threaten corporate information nor do they understand how these risks can be minimised.

In the past, the responsibility for information security appears to have been assigned to the information systems function within the organisation, rather than the owners and users of the information (Firth 1993; James and Coldwell 1993). Managers considered this reasonable as the information has predominantly been stored and accessed via computer systems. The security of the information in and around the

computer system was considered a technical matter, relating directly to the computer hardware and software installed, and was hence a task presumed to fall within the responsibility of the computing area. In addition, little or no consideration was given to the security of information outside of the computer system.

The responsibility for the implementation and operation of computer information systems in general has moved over time from the system engineers to the users. This is illustrated by trends in both hardware and software. For example, the decentralisation and networking of systems, plus the portability and ease of installation of equipment has put computer hardware within the reach of non-technical users. In addition, due to the sophistication of software and its ease of installation and use, there is now a computer on nearly every employee's desk. It is not uncommon for users to unpack and install computer hardware, load and install the software then run diagnostics and set up initial system parameters, with little or no help from the engineers.

Whilst users are gaining expertise and proficiency in these areas, the question of protection of the hardware, software and data has not been an integral part of this shift. Users are seldom involved in the process of planning or implementing the security to ensure the integrity, confidentiality and availability of corporate information and the related technology. The need for the responsibility for security to move with the technology has been voiced. The involvement of all personnel in information security is seen as crucial to overcoming resistance, raising awareness and encouraging co-operation and commitment from staff (Bergman 1991; Berleur 1999; Fagan 1993; Forcht 1994; Hoppe 1994; UK Audit Commission 1994, 1998).

1.2 OVERVIEW OF THE RESEARCH TOPIC

The key theme of this research is the planning and management of information security and in particular, the research focuses on the involvement of information stakeholders in this process. The main objective of the research is to study the ownership of, and acceptance of responsibility for, information security measures by stakeholders having an interest in that information.

In the context of this research:

- Integrity means only authorised parties can carry out modifications in authorised ways, (Pfleeger 1997, pp5-6),
- Availability means assets are available to authorised parties, (Pfleeger 1997, pp5-6),
- Confidentiality, or secrecy, means the assets of a computing system are accessible only by authorised parties (Pfleeger 1997, pp5-6),
- Information security is ensuring the integrity, confidentiality and availability of information,
- A stakeholder is an owner, author, custodian or user of information or asset,
- Ownership is having a proprietary interest in the information or asset,
- Responsibility is the state of being answerable or accountable for information or assets within one's power, control or management.

1.3 OVERVIEW OF THE RESEARCH APPROACH

The research reported in this thesis was carried out in two stages (see Figure 1.1). During the first stage current literature and publications on security management were reviewed and a study of the state of security management in practice within Australian organisations was carried out. A case study approach was used to investigate the security of the computing environments within sixty Australian organisations with each organisation viewed as a separate case study. Data was collected via interviews with management and staff, and semi-structured observations of operations and premises. Each organisation's security management measures and procedures were reviewed and rated on a Likkert scale. Current security problems and potential problem areas were identified and also rated on a Likkert scale. Univariate and multivariate statistical analysis was carried out on the data collected with the findings from stage one providing direction for the development of a new planning and management approach in the second stage.

The security review resulted in a number of observations. These included generally poor implementation of protective security measures, low awareness of security

related risks and available countermeasures, lack of assignment of responsibility for security, and lack of stakeholder involvement in the planning and management of information security. The results of this study also portray marked shortcomings in the implementation of information security measures within organisations in the health care industry. In addition, an analysis of current security planning and management models found these to be inadequate for contemporary information environments, due to their technical emphasis and lack of stakeholder involvement.

These findings provide a backdrop for stage two of the research. Stage two consisted of the development of a new approach, the Orion Strategy, and the study of its practical application into an organisational situation. Based upon the Soft Systems Methodology, the Orion Strategy incorporates a high level of user participation. A dominant feature of the new approach is that security related problem situations existing within business organisations are, in effect, handed back to the people who use, and are responsible for, the information. This strategy is a tool to enable those people, with the aid of technical advisers, to develop, implement and maintain feasible and appropriate security solutions to which they are committed.

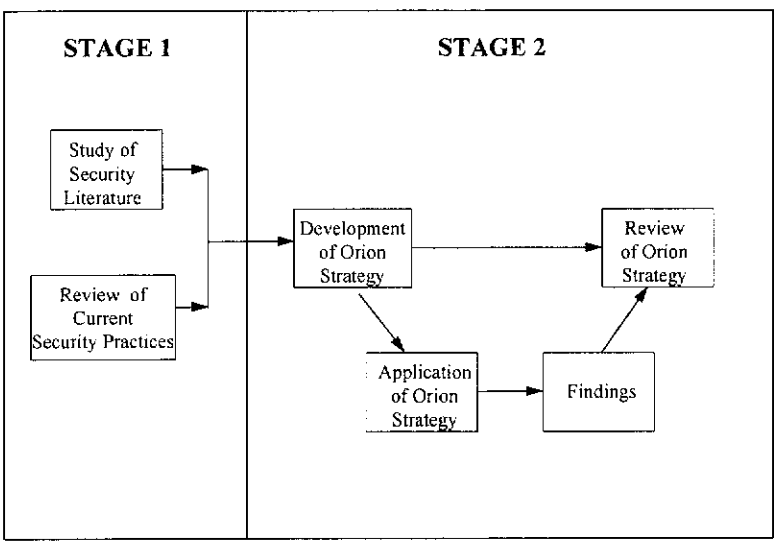

Figure 1.1: Stages of the Research

Action research was used to apply and refine the Orion Strategy within a large private hospital in Western Australia. The new method was developed further as it was applied in practice and learning was gained from this experience. The findings from this exercise related to both the content of the new model as well as the process of its application. The original Orion Strategy model was then reviewed for its suitability and adaptability to the situation under study.

1.4 STRUCTURE OF THE THESIS

The thesis is divided into nine chapters. Chapter 2 justifies the need for the research into information security planning and management. This chapter is a summary of an extensive literature search with the need for more active information security management appearing as the emerging theme. Chapter 3 details current security management models and techniques, ranging from highly theoretical and technical models through to more practical, user-oriented models.

Chapter 4 describes the research methodologies used. More traditional quantitative methods predominate in the early part of the research. The building of the new model and the learning from its application use qualitative methods. Chapter 5 summarises a security study conducted in Australian organisations undertaken as the first part of this research. This study was designed to ascertain the levels of implementation of security measures and identify any gaps in the security planning and management processes.

Chapter 6 explains the original Orion Strategy model as first devised. This model was then revised during the practical application stage detailed in Chapter 7. Findings from the research are discussed in Chapter 8 together with recognition of the limitations to the research. Finally, Chapter 9 summarises the research as a whole and discusses areas of possible future research.

2. JUSTIFICATION FROM THE LITERATURE

2.1 CHAPTER INTRODUCTION

This chapter discusses the risks to information security and looks at current trends in the management of security within business organisations. This section summarises the literature from the past decade to give an overview of the state of information security management in organisations. One of the main areas covered relating directly to the research theme is the assignment of responsibility to information owners, custodians and users. The chapter concludes with the needs arising from the current state of information security within the international community and recommended management action in order to achieve the aims of information security.

2.2 THE RISKS TO INFORMATION SECURITY

The aim of planning, designing and implementing security in and around computerised information systems is to ensure not only the *integrity* and *confidentiality* of information produced and used but also the continued *availability* of the information and its associated computer systems (Davies 1986; Forcht 1994; Gasser 1988; Parker 1981; Pfleeger 1997).

The scope of information security in this thesis encompasses not only information stored on computerised systems, but also organisational information used in manual processes outside the computerised environment. Hence information security deals not only with the computer systems storing and processing the information, but also the environment in which the information is created and used. Hence information security has a much broader scope than purely information systems security.

Threats are actions or circumstances affecting information systems assets (hardware, software and data) which have the potential to cause loss. Loss can result from processes of modification, erasure, interceptions, fabrication, destruction, damage, theft, leakage, interruption and denial of service. Such occurrences spring from both

intentional and unintentional actions. Intentional acts include fraud, theft, hacking, viruses, unauthorised access, industrial espionage and sabotage. Unintentional actions cover acts of God such as earthquakes, fire, flooding, storms; and accidents such as burst water pipes, motor vehicle, train and aircraft accidents, etc. Due to their random nature, unintentional acts are more difficult to predict and to eradicate the associated losses. However, effective planning and management is needed to minimise the effects of intentional acts.

The following list details the processes causing loss as a result of intentional and unintentional acts. The list as presented is a combination of many authors' work, however, the major sources only are cited at the end of the list:

1. *Modification* can occur to stored data, hardware, software and transmissions via human error, acts of God, fraud, hacking and the like.
2. *Destruction* affects hardware, software, data and transmissions and can occur through sabotage, hacking, human error, accidents, acts of God and viruses.
3. *Fabrication* applies to data and transmissions, mainly from acts of industrial espionage, hacking and fraud.
4. *Disclosure* occurs from leakage of data and transmissions, unauthorised access, industrial espionage and hacking.
5. *Interruption* and *Denial of Service* can affect hardware, software and data via acts of hacking, industrial espionage, viruses, acts of God, accidents and human error.
6. *Theft* of hardware, software and data can occur through acts of hacking, industrial espionage, copyright infringement and the stealing of physical property.

(Baskerville 1988; Carroll 1996; Pfleeger 1997).

In order to manage these threats effectively, management must understand the character of the threat and the possible outcomes these pose to the corporation's information asset. Information protection is defined as "the protection of, and recovery from, unauthorised disruption, modification, disclosure or use of

information and information resources, whether accidental or deliberate" (DeMaio 1992, p.xv).

This research concentrates on the planning and management of security to minimise intentional acts of abuse, however, the approach developed would also assist in the minimisation of problems emanating from human error and accidental occurrences. The following subsections highlight the absence of such a cohesive approach in current business practice.

2.3 CURRENT STATE OF INFORMATION SECURITY FROM THE LITERATURE

2.3.1 Reliance on I.T. and its Fragility

Management's reliance upon computer systems has increased dramatically as technology has developed. Over the past two decades in particular, the nature of computing has changed, becoming an integral part of business processes. Information has developed into a strategic asset, and the associated computerised information systems have become strategic tools for the organisation (Earl 1988; Frenzel 1992; Keen 1988a; King 1994; Porter 1980; Schultheis and Sumner 1995). Information is now critical to business operations and decision making activities allowing organisations to survive and prosper in competitive and tight economic environments. Unfortunately, mission critical applications are being exposed to greater security risks as organisations push their technological resources to the limit in order to meet organisational needs (Marro 1995).

As discussed at great depth in their book, Forester and Morrison (1990, p.vii) state that "computer systems by their very nature are insecure, unreliable and unpredictable". Management has applied the sophistication of technology without due regard to the shortcomings and risks inherent in its application. The advances in technology have produced powerful and complex hardware and software tools, but the development of security tools sadly lags behind. "Each major technological advance in computing raises new security threats that require new security solutions,

and technology moves faster than the rate at which such solutions can be developed" (Gasser 1988, p8).

The linking of computers and communications is seen by management as a leap forward, and all too commonly considered only in terms of its advantages. Angell (1993) remarks that technological monsters are being launched into our society by technocrats, businessmen and politicians in the arrogant belief that because they initiate a system, they somehow control its evolution and its resultant effects. He goes on to state "The short-sighted leading the blind! Commercial and social pressures, cultural incompatibilities, chaotic changes, resistance to change, unpredictable accidents, criminal intent, malice and sabotage add to the already excessive complexity, and can have surprising effects on what are usually considered technological decisions" (Angell 1993, p383).

Organisational strategies are changing, and businesses are altering their management structures and work patterns in order to harness technology to its greatest advantage. Information technology management trends such as downsizing, outsourcing, process re-engineering, distributed architectures and client/server all include an orientation towards making organisations leaner and more efficient. However, management needs to recognise the risks associated with these technologically-based solutions.

The risk of abuse increases as systems and processes become more distributed and decentralised. The more thoroughly computerised and networked an organisation is, the greater the risk it faces when initially connecting to the outside world (Wallich 1994). Systems are more difficult to monitor and control and many of the security mechanisms previously in-built in the earlier mainframe systems are no longer essential features. Networks are wide open spaces, and due to the general lack of controls intruders are now a major threat to networks, due largely to "a global economy that has turned businesses into electronic hubs on a vast electronic skein" Garner (1995, p33).

Unfortunately, basic security procedures are often overlooked in the redesign of the work environment, or the importance of security is under-rated. The changing

structure of organisations also has direct implications for security. For example, the removal of the middle management layer in a bid to trim the excess from administrative configurations has altered traditional control processes. "As organisations become leaner and fitter using technology to reduce layers of management, they run the risk of removing the controls and checks which former supervisory and managerial positions would have applied" (UK Audit Commission 1994, p12). In fact, the essential nature of previous controls in general has changed in this battle for efficiency. What was previously a mandatory security procedure often becomes an operational suggestion, at best implemented whenever employees remember security procedures (Clay 1995). The further one moves away from the mainframe, the less robust is the security software and, perhaps more importantly, the security culture (Paliotta 1995).

Global communications and the information superhighway are luring management into believing that easier and wider access to information will increase their organisation's performance and possibly gain a leading edge. Eugene Spafford, an internationally recognised security expert and author claims "People are seeing the glitter and the glamour of the information highway, but they don't see the risk. The vast majority of people have never really bothered to think carefully about what they may have to lose and what exposure they are taking for themselves by connecting to the network" (Markoff 1993, p.D1).

This trend towards telecommunications solutions is also changing the structure and culture of organisations. Angell (1995a) presents the view that these advances in telecommunications, the so-called information superhighways, are forcing a new order (which he suggests many will call disorder) upon an unsuspecting world. The quality and integrity of the information systems (and not just the data) is critical to economic survival - information must be delivered any place, any time, any how. He then states "global enterprise will require a substantial and redesignated security input in order to maintain coherence and cohesion of the transient organisation, to protect both the network and intellectual property, to prevent fraud, and to keep the discovery of new business opportunities secret for as long as possible." (Angell

1995a, p10). Hence management needs to recognise the threats associated with computerised systems and embrace a means of minimising the associated risks.

2.3.2 Increase in Computer Abuse

One of the indicators of the level of effective security management is the rate of computer-related crime and abuse. Computer crime has been defined by the United States Department of Justice as "any illegal act for which use of computer technology is essential for its perpetration, investigation or prosecution" (Parker 1983, p23). Computer abuse is defined as "any intentional act associated in any way with computers where a victim suffered, or could have suffered, a loss, and a perpetrator made, or could have made, a gain" (Parker 1983, p17).

It is extremely difficult, if not impossible, to estimate the true extent of corruption and crime currently suffered by organisations due to intentional computer misuse. Many sources suggest that the majority of computer crime is not detected, some estimating a detection rate of less than 1% (Jackson 1986). A definitive dollar value attributable to computer crime or abuse is also difficult to estimate. At the launching of an Australian Commonwealth inquiry into fraud in government in 1986 the Federal Special Minister of State, Mick Young, stated "figures ranging from $5 billion to as high as $30 billion have been cited. These figures could be exaggerated. The simple fact is we don't know" (Targetting Fraud 1989).

Ernst and Whinney submitted a study to the US National Commission on Fraudulent Reporting, reporting 80% of US companies questioned also suffered losses in the previous two years from computer security problems (Stemman 1987). More than half of these organisations had been victims of computer fraud. Protective measures in these organisations were reported to be either inadequate or non-existent.
A study by the National Computing Centre (NCC 1994) in the UK also found 80% of respondents had suffered at least one security breach over the two year period studied. A more recent UK study found 45% of participating firms experienced losses from computer abuse and fraud (UK Audit Commission, 1998). The 1999

annual FBI survey reports 62% of respondents suffered computer security breaches within the past twelve months (Power 1999). A previous survey by the FBI reported 64% suffered security breaches in 1998, an increase of 16% over 1997 and a 22% increase over 1996 (Power 1998).

A further study carried out by Michigan State University in the USA reported 72% of participating organisations experienced theft or attempted theft of money (Listen: computer crime victims speak ... 1995). Hancock (1999) reports 75% of organisations surveyed suffered losses due to security breaches in the form of either fraud, information theft or sabotage. The high rate of abuse occurrence appears to be similar over the past decade. Table 2.1 illustrates the percentage of organisations reporting losses from security breaches or computer crime.

The amount of loss suffered from computer crime can be difficult to gauge, and estimates appear to vary greatly depending on the source and subject. Arbouw (1993) estimates that workplace fraud is costing Australian business about $15 billion per annum. White-collar crime in the USA is estimated to be in the vicinity of US$200 billion per annum (Bequai 1998, Stern 1993).

Fraud alone costs businesses in the USA approximately US$120 billion per year (Arbouw 1993) and Donn Parker, adviser to the US Justice Department, estimates that "computer crimes cost the United States between US $50 million and $500 billion annually" (Marro 1995, p21). A summary of estimated losses from different types of computer crime is illustrated in Table 2.2.

Cases reported to the Australian Computer Abuse Research Bureau (referred to as ACARB), the official body for collecting and publishing information on computer abuse in Australia, had much lower average losses than those reported by the FBI. The ACARB research details a total of just under AUS$17 million in losses from computer abuse for the eleven year period 1980-1991, with the average loss being AUS$93,933 (Kamay and Adams 1992). The average loss from computer fraud in Australia, the category with the largest losses, was AUS$170,757. A further study conducted in Western Australia reported total losses of more than AUS$28 million

from only fifty-five cases of computer crime (James 1994a), the average loss being AUS$515,654. Table 2.3 summarises the average dollar losses from computer crime.

Year	% of Organisations	Involvement	Source
1987	80%	At least one security breach in the past 2 years	Stemman (1987)
1987	56%	Financial loss from computer crime (period not specified)	O'Donoghue (1987)
1993	44%	Financial loss from computer fraud in the past year	KPMG (1993)
1994	80%	At least one security breach in the past 2 years	NCC (1994)
1995	50%	Financial loss from security breaches in the past 2 years	Chidley (1995)
1995	72%	Financial loss from computer fraud (period not specified)	Listen ... (1995)
1995	75-95%	Suffered from acts of industrial espionage (period not specified)	Listen ... (1995)
1996	52%	At least one incident of fraud in the past year	KPMG (1996)
1997	62%	At least one incident of fraud in Canada in the past year	KPMG (1997)
1997	75%	At least one security breach (period not specified)	Hancock (1999)
1998	45%	Experienced losses from computer crime and fraud (period not specified)	UK Audit Commission (1998)
1998	64%	At least one security breach in the past year	Power (1998)
1999	57%	At least one incident of fraud in Australia in the past two years	KPMG (1999a)
1999	57%	At least one incident of fraud in Canada in the past year	KPMG (1999b)
1999	62%	At least one security breach in the past year	Power (1999)

Table 2.1: ***Percentage of Organisations reporting losses from security breaches or computer crime***

The continual rise in the rate of computer related crime is evident. Computer abuse in the form of fraud in Australia has risen by more than 500% in the decade 1980-1990 (Kamay and Adams 1990). The Audit Commission in the UK reported an increase of 183% in the total value of reported incidents in the 1990-1993 period (UK Audit Commission 1994). According to the Computer Security Institute in San

Francisco, the number of security incidents rose 73% from 1992 to 1993 (Garner 1995).

Year	Estimated $ Loss	Type of Crime	Country	Source
1986	$5 - $30 billion p/a	Fraud	Australia	Targetting Fraud (1987)
1993	$15 billion p/a	Fraud	Australia	Arbouw (1993)
1993	$120 billion p/a	Fraud	USA	Arbouw (1993)
1993	$200 billion p/a	White Collar Crime	USA	Stern (1993)
1995	$50 million-$500 billion	Computer Crime	USA	Marro (1995)
1998	>$200 billion	Computer Crime	USA	Bequai (1998)

Table 2.2: Estimated $ loss from different types of computer crime

Year	Average $ Loss	Type of Crime	Country	Source
1983	US$37,250	Computer Crime	USA	Stemman (1987)
1987	US$600,000	Computer Crime	USA	Stemman (1987)
1980-1991	AUS$93,933 AUS$170,757	Computer Crime Computer Fraud	Australia	Kamay and Adams (1992)
1994	AUS$515,654 AUS$3,021,155	Computer Crime Computer Fraud	Australia	James (1994a)
1997	US$957,384 US$954,666	Computer Fraud Theft of Information	USA	Power (1999)
1998	US$388,000 US$1,677,000	Computer Fraud Theft of Information	USA	Power (1999)
1999	US$1,470,592 US$1,847,652	Computer Fraud Theft of Information	USA	Power (1999)

Table 2.3: Average dollar losses from computer crime

The FBI reports that the most significant losses in the 1999 survey emanate from computer fraud and theft of proprietary information (Power, 1999). The average loss in the US back in 1983 resulting from computer fraud was reported at approximately US$37,250, whilst an average of US$6,270 was reported for ordinary theft (Stemman 1987). This compares with a study by the FBI claiming the average computer fraud loss in the US in 1987 was approximately US$600,000 compared with US$23,000 for manual fraud (Stemman 1987). The average loss from computer fraud in the US in 1999 is reported to be US$1.47 million (Power, 1999).

Industrial espionage is a growing industry, possibly due to the changing and competitive nature of the global marketplace. A decade ago industrial espionage in the USA was reported to be a $US20 billion per annum industry (Targetting Fraud 1989), and constantly on the rise. Espionage is estimated to have cost business US$250 billion in the past year (Hancock, 1999). Unauthorised access to computer files ('snooping') occurred in 95% of organisations studied by Michigan State University (Listen: computer crime victims speak ... 1995). The same research also reported 81% of organisations experienced theft or attempted theft of client information and more than 75% were victims of theft of trade secrets, new product plans and product descriptions. A USA study reported 56% of participating organisations discovered at least one attempted theft of intellectual property during the previous year (Hancock, 1999).

The Chief of the US Department of Justice's Computer Crime Division claims "Four years ago, the notion of paid attackers was very rare. Now we see people posting shopping lists for information inside hacker bulletin boards" (Garner 1995, p33). With the rise in technology education and availability and power of personal computers, the expertise and means to carry out acts of abuse is readily available. Techniques to accomplish computer crimes are not only well developed, but it is also easier to find people to assist with these acts. "Today there is a readily available talented pool of unemployed (downsized) technical experts as well as ex-KGB/Stasi communications and cryptology specialists who are seeking job opportunities. The computer crime problem will become more serious as opportunity, motivation and means become more readily available" (Sherizan 1995, p15). Computers are

welcome tools for industrial spies because they can not only provide large amounts of relevant information from selected victims, but also offer a low risk of detection with little evidence that information has been stolen and an easy route to convert stolen information into analysed intelligence (Sommer 1993).

The majority of the studies cited above include both public and private organisations, however, government departments and agencies have been the focus of additional and separate security reviews. According to Australian figures released by the Federal Police Association a security assessment of 438 Australian government agencies found 80% to be at risk of computer abuse (Targetting Fraud 1989). In addition, the same publication reports tax fraud amounted to $10 billion per annum, social security fraud $2 billion, defence fraud $800 million and health and medical fraud $700 million per annum.

In the USA the problems are similar, and the security of government department computer systems has also been found questionable. In 1994 the US Department of Defence hired a 'tiger team' of experts to run a penetration test on its own computer systems, a total of nearly 9,000 servers and mainframes. Using a series of surreptitious probes the tiger team managed to break into 7,860 or 88% of the computer systems (Garner 1995). Of those attacked, only 390 were detected and 19 attacks were reported to management by staff, supporting the view that organisations rarely know when they have been hacked. A survey conducted at INFOSECURITY '99 (Europe's largest IT security exhibition) found one third of government authorities had insufficient security measures to protect from hacking (Hancock 1999).

The character of abusive acts carried out using computers has changed as technology has advanced. Sophisticated telecommunications facilities have opened the door to problems such as hacking, unauthorised access and industrial espionage. Virus attacks have also spread more rapidly with expanding networks and communications.

Nearly 70% of the executives who took part in research conducted by Ernst & Young in the USA stated security risks have worsened in the last five years (Security 1995).

In the KPMG studies (KPMG 1993, 1996) over half the respondents stated they believed fraud is a major problem facing business, and that it will be more of a problem in the future, recognising the effect of economic pressures, the weakening of societies and the increasing sophistication of today's criminals.

The above figures indicate that computer crime is occurring, and that the rate is increasing. Computer crime is likened to the iceberg - the growing piece of ice protruding from the water indicates there is a problem, but the size of the iceberg below the surface is unknown (Carroll 1996, Power 1994).

2.3.3 Employee Involvement in Computer Abuse

The highest risk of computer abuse comes from employees within organisations according to the majority of the computer abuse studies carried out world-wide (Benbow, Masters & Cooper 1986; Kamay and Adams 1990 and 1992; James 1994a; O'Donoghue 1987; Straub and Hoffer 1988). Personnel within an organisation have knowledge of procedures, where assets are held and how, if at all, they are protected. Many crimes are committed by disgruntled employees (Stern 1993). These may include employees who have been passed over for promotion, awarded low pay increases (if any), or those who feel they are disliked or mistrusted because of their politics, background, religion, education or colour (Smith 1970).

The internal threat is certainly supported by many investigations into computer crime over the past decade in particular. In the KPMG (1993) study of Australian organisations the largest category of perpetrator was internal staff. This study reports 63% of fraud is committed from within the organisation, 25% from outside, and the remaining 12% by a combination of both internal and external sources. The James (1994a) study reported more than 60% of offences were carried out by internal staff. Similarly, ACARB reports that internal personnel were responsible for 92% of cases where the perpetrator could be identified (Kamay and Adams 1992). Benbow, Masters and Cooper (1986) found staff involvement in computer crime was as high as 87.5%.

The picture is very similar outside Australia. According to the National Centre for Computer Crime Data in California USA, 85% of computer and network break-ins were committed or aided by insiders (Rothfeder 1993). The FBI surveys state the internal proportion source of reported attacks are 88% in 1998 (Power 1998) and 80% in 1999 (Power 1999). In a Singapore study, employees were responsible for all cases of reported computer abuse (Seah et al. 1991). Employees are said to account for 65%-85% of fraud cases in the USA and up to 25% of the workforce from the upper levels down have seen opportunities for fraud on a regular basis (Targetting Fraud 1989). Weiss (1992a) suggests that management look inside their organisation for computer crime culprits for between 78% and 90% of all reported abuse comes from inside. Weiss also reports two-thirds of these perpetrators hold upper management positions. A survey by Ernst & Young (1998) reports that the highest risk internally comes from unauthorised users on the network, authorised employees, former employees and contract workers. Other "trusted" users quoted as high risk by Ernst & Young include authorised suppliers, consultants and customers. The extent of employee involvement in computer crime is summarised in Figure 2.4.

Year	% Employee Perpetrators	Type of Crime	Country	Source
1986	87%	All types of computer crimes	Australia	Benbow, Masters & Cooper (1986)
1989	65-85%	Computer fraud	USA	Targetting Fraud (1989)
1990	100%	All types of computer crime	Singapore	Seah et al. (1991)
1991	92%	All types of computer crime	Australia	Kamay and Adams (1992)
1992	78-90%	All types of computer crime	USA	Weiss (1992a)
1993	60%	All types of computer crime	Australia	James (1994a)
1993	63%	Computer fraud	Australia	KPMG (1993)
1993	85%	All types of computer crime	USA	Rothfeder (1993)
1998	88%	All types of computer crime	USA	Power (1998)
1999	80%	All types of computer crime ('likely source of attack')	USA	Power (1999)

Table 2.4: Extent of employee involvement in computer crime

There appears to be a high portion of cases where organisations have detected a computer crime, but are not able to identify the perpetrators responsible. In the ACARB (Kamay and Adams 1992) survey, 60.5% of organisations reporting cases were unable to identify the culprits responsible for abusive acts. This accounted for $5.6 million of reported losses. Again, perpetrators in the James (1994a) study were unable to be identified in 26% of cases, accounting for more than $800,000 in losses. The 1999 FBI survey reports perpetrators could not be identified in 29% of cases (Power, 1999). These figures clearly indicate that current detection methods implemented by management are inadequate.

Estimates of losses from computer crime vary significantly, but computer fraud carried out by internal employees should be of major concern to management. Hartley (1993) suggests that if your organisation has not suffered from computer fraud, either it happened but you don't know about it, or you have just been lucky. Most managers feel they can trust their employees, however Menkus (1991, p293) states "trust building as a basis for organisational effort in inherently deceptive, since all fraudsters, embezzlers, organisational spies and resource wasters are trust violators by definition". Regarding the honesty of employees, an FBI Officer stated 'in every office, 10% of the people are completely honest, 10% are completely dishonest, but the remaining 80%, well it just depends on the situation' (Fitzgerald 1991, p41). The need for managers to protect their computer systems against 90% of their employees is certainly a daunting task!

2.3.4 Current Level of Information Security Management

Management generally is not cognisant of the threats inherent in the use of computerised information systems (Forester and Morrison 1990; Pfleeger 1997). When the UK Audit Commission reported its first survey more than a decade ago, it noted that the opportunity to commit abuse existed because of a lack of basic controls, rather than particularly sophisticated manipulation of procedures. "Now, as then, opportunities are still widespread and weaknesses well-known, but for a variety of undisclosed reasons, management do not impose adequate controls" (UK Audit Commission 1994, p4).

Criminals need to have a good knowledge of computer systems, a detailed knowledge of the business activities of the targeted organisation, an opportunity to carry out a criminal act via some security hole or area of vulnerability, and some motivation to carry out the crime. Motivations include greed, revenge, the need for a challenge, or basic curiosity. Employees working with computer systems will develop a good knowledge of these systems and the business procedures around them. A lack of security both in, and around, computer systems provides the criminal with the opportunity for abuse. "Ad hoc security measures provide, at best, insignificantly increased protection that rarely justifies their expense. At worst, they provide a false sense of security that renders the users more susceptible than ever to the real threats." (Gasser 1988, p10).

In the past, it appears that security of corporate information has not been high on the management priority list in Australia. In a report to parliament, the WA Auditor General highlighted the lack of data security in government departments, stating that basic security measures were neglected, state government security guidelines ignored, and information not adequately protected from unauthorised manipulation, disclosure or loss (OAG 1992). Research into security management within other Australian organisations has reported similar findings over the past decade (Benbow, Masters & Cooper 1986; James 1994a; Kamay and Adams 1992; KPMG 1993). These studies conclude that basic security measures are either lacking or ineffective in the majority of organisations studied.

During the 1980's corporate corruption was a widespread problem in Australia. Ethics was overshadowed by greed and power play (Middleton 1992; Southee 1992; Stannard 1993) and the IT area was not removed from unethical decision making (Benton 1986; Cameron 1993; Thomsett 1993). Although the need for higher ethical behaviour in IT and business is recognised, the Criminal Justice Commission (1993) suggests we have a unique problem in Australia. Deeply embedded in our culture are myths that apparently make it harder to prevent corruption. One myth is that fraud against government is a victimless crime and therefore is not really a crime at all. Government organisations are faceless bureaucracies, and to defraud the government

is more a sport or battle of wits, even if it is a violation of the law. Another myth is it is un-Australian to "dob in a mate" or inform on a friend. Australian 'mateship' appears to be a unique relationship, emanating from convict settlements in early Australian history. Managers also believe that 'there is no corruption in my organisation'; and violators believe 'I won't get caught'. Unfortunately it takes time to eradicate beliefs that are embedded in culture.

However, the lack of adequate security management is not a problem confined to Australian organisations. Sherizan (1995) reports, there is a lack of minimal security protection in the West in general and even more so in many other parts of the world. The USA reports similar problems of inadequate controls. A study completed by Coopers and Lybrand (1988) on the security of networked systems found that the level of security achieved by the 44 organisations studied was inadequate. Garner (1995, p36) reports "despite the warnings of the security community, the increasing number of attacks, and the rising costs of losses, most US companies still refuse to implement adequate security controls".

The UK Audit Commission (1994, 1998) found the primary reasons for computer abuse were disregard for basic control safeguards and ineffective monitoring procedures. It further reported an absence of positive action for minimising the risk of computer abuse, particularly given the high degree of dependence upon IT by most of the participating organisations. In particular, it found that approximately 65% of organisations had no security awareness training in place, 82% practised no risk analysis, 85% had no staff responsible for security and more than 95% had inadequate personnel screening. Smith (1996, p197) suggests that organisations within the health industry in the UK and Europe do not comply with the UK Data Protection Act when he states "at present many patient records breach the data protection principles; many are inadequate, irrelevant, and excessive, and organisations fail to ensure their accuracy, completeness and currency".

The European Security Forum (1995a) examined the reasons behind the security breaches reported in their 1994 survey, finding the most common cause of security incidents is negligence, with 24% of respondents suffering significant impact to their

business through loss of availability, confidentiality or integrity of proprietary information. This research also found local area networks, end-user computing and corporate communications networks are not effectively addressed within corporate security policies and many organisations have unsatisfactory risk analysis processes, resulting in security controls that are potentially ineffective or inappropriately applied.

A "seat-of-the-pants" approach to security has been common in organisations. Management has responded to security issues only when a violation has been experienced and even then, solutions have been fragmentary in nature with no holistic or corporate-wide risk view considered. Hoffer and Straub (1989) report "there is evidence that many firms do not introduce security measures until a major abuse has occurred; this pattern, obviously, is reactive rather than proactive". Seah et al. (1991) reported a short-term, piecemeal approach to computer security in the majority of participating organisations, characterised by the use of basic, low cost security measures, frequently in response to a security violation. Information security activities undertaken by large organisations tend to be autonomous, fragmented and isolated (Smith M. 1998). Unfortunately, in many cases security violations are just swept under the carpet (David 1995).

Abrams and Moffett (1995) suggest that traditional computer security "reacts to events" and more effective security in distributed systems entails taking a more active and positive stance. They argue that security of information is much broader than currently viewed and requires a proactive management approach. However, rather than invest resources in preventative protection, there tends to be a more reactive approach to security. Vulnerabilities are not recognised as security problems until a violation occurs.

The increased vulnerability of organisations via their computer systems is highlighted in many studies. As organisations become increasingly dependent upon IS, there is greater risk from disclosure, destruction and alteration of data, and disruption of information services (Dickson et al. 1984). Watson (1989) warns against the risk of

making faulty business decisions due to discrepancies amongst different data sources due to lack of controls in IS and user departments.

Very few studies report adequate or better levels of management of information security in the majority of participating organisations. Unfortunately, it is difficult to compare these studies because dissimilar criteria are used to measure adequacy. However, the respective criteria used in each study appear appropriate to indicate some measure of adequacy, and the findings indicate that the current state of security management is inadequate.

2.3.5 Security Awareness, Ownership and Responsibility

One factor contributing to the inadequacy of controls currently in place within organisations could be a lack of awareness of security risks and the value of the organisation's assets. Whilst many firms recognise the value of their information assets and have applied appropriate protection, other organisations are dangerously deficient in their security measures. "But, unlike the 'wild west' bankers, some computing professionals and managers do not even recognise the value of the resources they use or control." (Pfleeger 1997, p2).

Computer security studies both in Australia and worldwide continually report the low awareness of management with regard to threats to the security of the corporation's information systems. There is still the prevalent attitude that it won't happen to us (Benbow, Masters & Cooper 1986; Gardner 1989; Kamay and Adams 1990; Forester and Morrison 1990).

Senior managers are gradually becoming computer literate, but few are technically skilled in computing and fully understand the risks associated with computer systems. Awareness generally increases with knowledge and its application. The sensationalism of high profile computer crimes (such as hacking and viruses) by the media has helped raise a general awareness of a limited range of threats. However, McCusker (1994) believes that many people feel the ideal security solution has not yet been invented due to apathy on the part of people who should be concerned with

security. The lack of awareness of senior executives in both the private and public sectors toward computer crime and security has been noted and it has been suggested that either the indifference managers currently have towards security concerns will disappear, or the executives will (Targetting Fraud 1989).

It is a little surprising to find, however, that most executives responding to a study on fraud by KPMG (1993) considered themselves to be knowledgeable on how fraud could occur, though approximately one third of the respondents reported that there was evidence of the existence of the fraud experienced, but this was either ignored or not acted upon quickly enough. Security education is essential in order to raise the awareness of security issues. The absence of security awareness training and security education has been reported by many security studies (Benbow, Masters & Cooper 1986; James 1994a; O'Donoghue 1987; UK Audit Commission 1994, 1998).

A further problem evident in many studies is the lack of responsibility assigned to, and accepted by, employees. Security professionals have continually recommended that overall responsibility for information security be assigned to a manager and each employee be responsible for security in their area of work. The lack of security supervision and assigned responsibility for information security has been noted in several security studies (Dhillon and Backhouse 1994a; Security 1995; UK Audit Commission 1994, 1998).

Unfortunately, when it comes to information security Menkus (1991, p295) states "what is everyone's responsibility really is no one's responsibility". Dhillon and Backhouse (1994b) state there is a reluctance on the part of users to deal with IT security risks. James and Coldwell (1993) found that information security was "inherited" by technical and operational IT staff, not by design, but by default in the majority of participating organisations. Further, often a person assigned responsibility for security does not have the necessary means to discharge it adequately because the relevant powers have been assigned elsewhere (Backhouse and Dhillon 1993).

Security is the responsibility of all employees, but it needs to be managed. Security measures need to be 'owned' by trusted staff members who must monitor and

administer them to the point where management asks "whose job is on the line if this control fails?" (Parker 1998:21).

In the past, mainframe systems had in-built security mechanisms and IT staff were responsible for controlling procedures in and around the computer. Security mechanisms were automatically carried out either by the computer itself or by supporting staff in computer processing procedures. However, IT personnel no longer have control over information security mechanisms, and users are reticent to accept responsibility. "In the corporate world, information security its generally seen as being of interest to the IT department, and so many professionals do not give adequate importance to these security concerns of an organisation" (Backhouse and Dhillon 1995, p2)

However, minicomputers, networks and distributed systems have only remnants of the core security mechanisms of their mainframe predecessors. As more computing power is distributed to users, security measures are moving from essential systems features to optional extras. Backups, logical access control, database management control, system logs, communications control and integrity checking are no longer primary security features. Superuser status can now be distributed and more powerful remote facilities are available within interconnected systems.

Many users also consider security procedures hinder their work performance. "Security measures often interfere with an honest user's normal job" argues Gasser (1988, p11). Alexander (1995) claims one reason some organisations are reluctant to implement proper security controls is due to management concerns that such controls would hinder employee productivity. Inappropriate and over-secured work environments may also inconvenience users to such a degree that they won't use the system (McCusker 1994).

2.3.6 Importance of Information Security

Security awareness is in a state of transition, as management becomes more cognisant of computer crime and security issues with a realisation of the organisation's

susceptibility only just beginning to emerge. A decade ago authors were forecasting a rise in the importance of security matters (Jackson B. 1986). The ranking of security issues would change, based upon the trend toward PCs, LANs and end-user development according to Sprague and McNurlin (1986). These factors are making companies more vulnerable to electronic intrusion and abuse.

The growing importance of security to information systems managers is also illustrated by its inclusion as a key management issue in several opinion surveys undertaken over the past decade as indicated in Table 2.5.

Year	Issue	Rating	Country	Authors
1985	Security Backup	5	USA	Kanter (1986)
1985	Data Security	6	USA	Hartog & Herbert (1986)
1986	Data Security	11	USA	Herbert & Hartog (1986)
1990	Control & Compliance Mechanisms	11	China	Harrison & Farn (1990)
1991	Data Security	2	USA	Deans et al (1991)
1991	Improving Information Security and Control	19	USA	Niederman et al (1991)
1992	Improving Security and Control	2	Gulf Cooperative Council	Badri (1992)
1992	Data Security	9	India	Palvia & Palvia (1992)
1992	Quality of Input Data	3	India	Palvia & Palvia (1992)
1992	System Reliability and Availability	4	Hong Kong	Burn et al (1992)
1993	Improving Security and Control	5	Estonia	Dexter et al (1993)
1993	Security and Control	6	United Kingdom	Galliers et al (1994)
1993	Improving Data Integrity and Quality Assurance	7	Australia	Pervan (1993)
1993	Improving Information Security and Control	19	Australia	Pervan (1993)
1994	Security and Control	6	Poland	Wrycza & Plata-Przechlewski, 1994
1997	Security	Top 10	Australia	Gartner Group, 1997
1997	Security and Control	3	International	Watson et al (1997)

Table 2.5: Rating of Security as a Key Issue in Information Systems

The research findings reported by Kanter (1986) and Herbert and Hartog (1986) rate security at fifth and sixth in importance respectively. In 1990, a study in the Republic of China rated control mechanisms and compliance to standards at 11

(Harrison and Farn, 1990). Niederman, Brancheau and Wetherbe (1991) report security and control was rated at 19 in the USA, however a study of USA multinationals in the same year rated data security as second only to educating senior personnel (Deans et al. 1991). The quality of input data and data security were rated 3 and 9 respectively in research carried out in India (Palvia and Palvia 1992), and Hong Kong managers voted systems reliability and availability at 4 (Burn et al. 1992). In 1992 also the Gulf Cooperative Council (representing Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and United Arab Countries) rated information security and control second to improving IS strategic planning (Badri, 1992). Improving security and control was rated at 5 by Estonian managers in 1993 (Dexter et al. 1993).

Security was rated 6th in importance by managers in the UK in 1993 (Galliers, Merali & Spearing 1994) in addition to managers Poland in 1994 (Wrycza and Plata-Przechlewski 1994). Australian managers rated improving data integrity and quality assurance at 7 and improving information security and control at 19 (Pervan 1993). The Gartner Group (1997) report security as a concern in the top ten in Australia. An international study in 1997 by Watson, Kelly, Galliers and Brancheau ranked security and control at 3 (Watson et. al. 1997).

Galliers, Merali and Spearing (1994) considered not only the importance of issues to IS managers, but also how problematic each issue appeared to be, and although security and control was ranked 6th in *importance*, it was ranked only 19th as *problematical*. This would imply that those organisations included in the study believe security issues are very important and they are managing security issues satisfactorily.

The changing nature of technology and the business and economic environments in which organisations operate are continually altering the character of the threats to computerised information. The expansion of telecommunications and networking, in particular, has increased the opportunity for computer abuse and raised the profile of information security accordingly. A study of computer security professionals by Truman (1993) reports that network security is a major concern area. Although

information systems professionals have always recognised the importance of security measures, the increase in computer crime and abuse and the expansion of underground networks, has elevated security to a higher priority (Marro 1995).

2.4 EMERGING NEEDS

Although the above figures indicate an increasing concern about security issues, management still shows an ignorance of security issues and a lack of response to the apparent risks. It appears evident that security and control issues are, or should be, of concern to management. Numerous studies into security over the past decade indicate security management is sadly lacking and managers and users are not fully aware of vulnerabilities related to the organisation's information. This suggests current methods used to plan and manage effective and appropriate security measures, are inadequate.

Chantler (1992) claims that to really understand the organisation's vulnerabilities, managers must put themselves in the opposition's shoes and think like criminals. More than a decade ago Parker (1981) stated the rules of the game are made by the enemy, not the security specialist and it appears that the computer criminal still has the upper hand. Moore (1994) suggests the fear of tomorrow is the highly sophisticated and educated criminal who can wield the state-of-the-art technology to best advantage.

The above discussion indicates gaps relating to comprehensive and pre-emptive management planning and action, and an increased awareness of risk and security measures. It is also apparent that the inclusion of stakeholders in the planning and management of information security is rare.

2.4.1 Holistic and Proactive Management Approach

The need for a more holistic and proactive approach to planning and managing information security is a paramount consideration for organisations wishing to implement effective information security. The call for a more holistic approach has

emerged from numerous sources (see Angell 1995b; Dhillon and Backhouse 1994b; Hoffer and Straub 1989; NRC 1991; OECD 1992; Yngstrom 1995; Zuckerman 1998) and becomes more pressing as technology advances.

Security measures are implemented to protect organisational assets and ensure their integrity, confidentiality and continued availability. Unless security is appropriately aligned with organisational goals its effectiveness will be limited. "Security needs to be mapped into those business processes such that it supports properly the business objectives" (Collins and Mathews 1993, p16). Information security mechanisms must be pertinent to the organisation's objectives and activities, and their integration is necessary to ensure security is effective and appropriate.

A holistic view requires a comprehensive, organisation-wide security perspective to ensure a top-down approach to planning security. Such a view will ensure the vision is expansive and contains no omissions, and at the same time recognising the needs of different sections of the organisation. Yngstrom (1995, p98) states "In order to be able to cope practically with security ... security needs to be treated holistically". A holistic perspective will ensure piecemeal security solutions are not applied to isolated problem areas where no consideration is given to the integration and influence of other protective measures. Angell (1995b, p10) believes security should not be considered only in terms of technology, but "information systems must be treated in holistic terms, as social systems in which technology is only one element". He goes on to suggest the concept of security itself will have to be redefined to encompass these ideas, which will impact on all company systems.

A proactive stance entails planning and implementing protective measures before problems arise, rather than waiting until a security violation has occurred (Hoffer and Straub 1989; Jaehne 1984). To do this, management must be aware of the organisation's security risks, understand how solutions can be applied in the context of organisational goals, and be prepared to invest resources to take preventative action. This also requires an active distribution of responsibility for the security of information by stakeholders and ownership by stakeholders of that responsibility. In order to achieve this ownership, security and protection issues must be embedded

into the organisational culture and management mind-set. Such a stance would mean all employees are automatically mindful of security matters in their planning, managing and operational activities. Inclusion of security in the organisation's culture also requires security to be integrated into the organisation's activities rather than an isolated and separate exercise.

2.4.2 Raised Security Consciousness

The second major need arises from the poor state of security and current low awareness levels evident within organisations. This is the need for an increased security awareness in stakeholders and users at all levels. Heffernan, a consultant on national security affairs to the FBI claims "the challenge is to convince employees they can be part of the solution rather than part of the problem. Awareness is the key to protecting current and future competitiveness and jobs" (Engler 1995, p48). Practice has shown that when education programmes have been conducted and employees understand protective measures and why they have been implemented, rates of abuse are reduced and employees become more aware of security issues (Markey 1989; O'Donoghue 1987; European Security Forum 1995a).

The belief that security and technical systems concepts are too complex to be understood by non-IT personnel is incorrect. For example, the US Department of State have run extensive security training programmes for their staff at all levels and report that although computer operators and technicians may feel that systems concepts are too complex to be grasped by "non-technical" people this is not so (Markey 1989). It has been suggested that this belief may have emerged from the inability of IT people to explain concepts in non-technical terms (Corbin 1991; Kennedy 1994; McCoy 1994).

Security education must not only be conducted for isolated groups of employees, but for employees at all levels of the organisation. The European Security Forum (1995a) claims that situations where senior management is aware of the need to apply risk analysis to computer-based systems, the effectiveness of the security mechanism

throughout the organisation increases and security awareness campaigns are as important among senior management as among users and IT staff.

2.4.3 Greater Stakeholder Involvement

A further consideration is the need for involvement of the system owners, custodians and users in the process of planning, designing and implementing security within the organisation, to ensure these are appropriate and are integrated into the culture of the work environment. "Principles are quintessentially human and social attributes and the reason we are introducing them here is because the question of computer security is not per se a technical problem. It is a social and organisational problem because the technical systems have to be operated and used by people" (Backhouse and Dhillon 1995, p3).

In the experience of the researcher, information systems are generally structured, inflexible and non-social systems. They pay no heed to power and politics and their recognition of different groups of employees is limited to preset database 'views'. In addition, systems designers and developers generally lack a coherent and full understanding of the business situation and are seldom in a position to comprehensively identify business-related security loopholes and dictate solutions.

Many authors and researchers are beginning to emphasise the importance of security professionals working together with organisational employees at all levels in order to achieve a coherent and integrated information security strategy (Adams 1995; Backhouse and Dhillon 1993; Hitchings 1994 and 1995; Vaughn, Saiedian & Unger 1993). This is not always an easy task, as each employee has a unique view of his or her work environment, together with personal and political agendas. "Organisations are constantly influenced by culture, power and politics .... organisations are dominated by an informal environment. The boundaries of which are either fuzzy or so encompassing as hardly to exclude anyone. To analyse any managerial situation is thus problematic." (Dhillon and Backhouse 1994b, p1)

Achieving consensus among different stakeholders in an organisation regarding safeguards for an information system is more difficult than solving many technical problems (Backhouse and Dhillon, 1995). It is essential that the expertise and knowledge of senior executives, management, users and IT personnel be pooled to ensure the implementation of a cohesive and appropriate security strategy. The involvement of all relevant parties also increases the ownership felt towards strategies put into place, and are therefore more likely to succeed in the long run. This concept has been proven by the US Department of State where the effectiveness of the systems security program depends to a great extent on the participation of line managers, line security personnel and users (Markey 1989).

2.5 CHAPTER CONCLUSION

The reliance upon technology to produce accurate and timely information for decision making is increasing. However, the rate of technological advancement is much faster than the development of means to ensure the integrity, confidentiality and continued availability of information and systems. Although management is becoming more aware of security issues, the rate of computer-related crime and abuse is rising.

Awareness of security risks and available countermeasures is continually reported to be low in studies carried out over the past decade and security measures implemented within organisations to protect information are generally poor. Responsibility for security is seldom assigned and information owners, custodians and users are not held responsible for the security of the information they hold and use. The planning and management of information security is reported to be poor.

The needs seen to arise from this situation include a more comprehensive or holistic view of information security and its management, a proactive approach to the security of assets rather than a reactive stance, and programmes to raise awareness of security issues. A greater involvement of stakeholders in the planning and management of information security may also assist.

3. INFORMATION SYSTEMS SECURITY MANAGEMENT MODELS

3.1 CHAPTER INTRODUCTION

The previous chapter reports security management within business organisations worldwide is poor and needs attention. This chapter describes the tools currently available for the planning and management of security within organisations.

3.2 CURRENT I.S. SECURITY MANAGEMENT MODELS

There are a number of different types of models proposed for information security management. The content, structure and application of examples of the most dominant model types will be studied in greater detail. Each of the models included has been developed to meet a particular need and hence has a different purpose, structure, content and level of application. Different types of models have been devised for purposes such as the design of systems methodologies, analysis of cost-effectiveness of security actions, development of security technology, the review of security threats and security education and training needs (Smith 1993).

Traditional approaches to information systems security have a scientific core that has emerged from the engineering origins of computing. Methods used traditionally to manage information systems security generally focus on the technology and thus propose technical solutions. The majority of these methods utilise assessment practices and mathematical models to provide measurable results. These approaches seldom consider socio-technical, human and organisational factors.

The emphasis upon technical issues with relation to information systems security is evident from the wealth of complex, formula-based tools developed over the past two decades. Whilst technology is a necessary consideration, it is not the only element requiring recognition. Organisational concerns, human factors and social considerations also directly and indirectly affect the security management function (Baskerville 1988; Yngstrom and Bjorck 1999).

Technical considerations include computer hardware and software, electronic equipment and devices, and telecommunications facilities. Security relating to technical factors would include protection of stored and transmitted data by encryption, network firewalls and gateways, access restriction devices and the like. Also included are the security of telephone systems (eg PABX), electronic monitoring devices and authentication devices. Any device or consideration of a technical nature is included in this element.

Organisational factors include considerations at the strategic, tactical, and operational levels. Organisational strategies, structure and management style, organisational culture and policies, and politics are important at the strategic and tactical levels. Factors at the operational level include job designs, work flows and any practices associated with general operations. Baskerville (1988) suggests that organisational factors important to effective information security include awareness of security responsibilities for members of the organisation at all levels, the environment in which the organisation operates, the security program itself (i.e. policies, planning, education, etc) and the audit function for ongoing control and management. These are internal organisational factors.

External organisational factors relate to the environment in which the organisation operates. Environmental factors include regulations and statutory requirements imposed by law (for example, health and safety regulations, corporate regulations dictated by company law), physical environmental limitations, and constraints imposed by associated bodies (for example, Government Agencies, other business organisations).

The ***human*** side looks at behavioural aspects and considers the different perspectives of the people involved, i.e. the stakeholders or those who have a particular interest. Because human behaviour is difficult to predict, human-oriented situations and systems tend to be imprecise. People who are stakeholders of a given information system include owners of the system, people who use the system directly, people who rely on the system and people who design, build and maintain the system. The view of each stakeholder will differ. Personal politics and ambitions will also contribute

to each person's unique perception. Politics in this sense is power-related activity concerned with managing relations between different interests (Checkland and Scholes 1990).

The ***social*** environment within which the system operates is an important consideration. Social factors relate to influences such as roles and values. This includes societal, cultural and religious elements influencing the way a person thinks and acts. Social factors also include ethical influences (Kowalski 1994). For example, hacking and industrial espionage are a result of social influences emanating from the environment in which the organisation's information system exists. In addition, laws and statutory regulations relating to the protection and privacy of data form part of societal considerations.

Models and methods to assist in the planning and management of information security and information systems security have developed over time in response to apparent needs. These models differ in format, scope and methods of application, making direct comparisons difficult. However, all models can be evaluated for their recognition of technical, organisational, human and social considerations.

3.2.1 Classification of Models

There have been a number of classifications of practical and theoretical information systems security management models over the past decade (Dhillon and Backhouse 1994a; Smith 1993; Yngstrom 1996). However, the models found were generally complex, abstract and impractical. Information security models can be classified into five groups; *onion skin* models, *checklist* models, *matrix* models, *filter* models (Smith 1993), and *socio-technical* models (Kiountouzis and Kokolakis 1996). As this five class categorisation is the most comprehensive offered thus far, it is used in this research as a basis to describe the current models. Unfortunately, the criteria identifying a particular class of models is indistinct and classes do not appear to be mutually exclusive. Hence, each model has been placed in the classification reflecting the most dominant features of that model.

The security industry has a wealth of tools for the analysis of risk and cost-justification of security solutions. However, as these tools only address a limited area of information security management such models are not detailed as part of this research. Concentration will thus be focussed on total management models. Each type of model will be discussed in terms of their purpose, structure, content, application and their ability to integrate organisational, social, technical and human elements into the security management function.

3.2.1.1 Onion Skin Models

Onion skin models feature concentric circles or layers arranged around the data, akin to the layers of skin on an onion. These models are also referred to as 'ring' or 'layer' models and examples of this type of model can be found in Hussain and Hussain (1988), Lane (1985), Martin (1973), Parkinson and Paul (1989), Saddingham (1988), and Vasarhelyi and Lin (1988). The purpose of onion skin models is to explain the affect of actions and environmental factors on the computer systems and their core data. The structure of an onion skin model is illustrated in Figure 3.1. Numerous layers are built around the core data, each layer denoting an action or environmental factor that could effect this data.

The content of the onion skin model differs with each interpretation presented, however, one common element is the central data and/or computerised information system. The surrounding layers can illustrate security controls or actions relating to business activities or organisational structure (Lane 1985; Martin 1973; Parkinson and Paul 1989).

A useful feature of this type of model is that it emphasises the role of various types of action in providing the context for other types of action (Smith 1993). This also places the security object into context by giving guidance for controls and types of safeguards forming the security boundary and where this boundary be placed. Unfortunately, there are no application guidelines or implementation tools associated with this type of model.

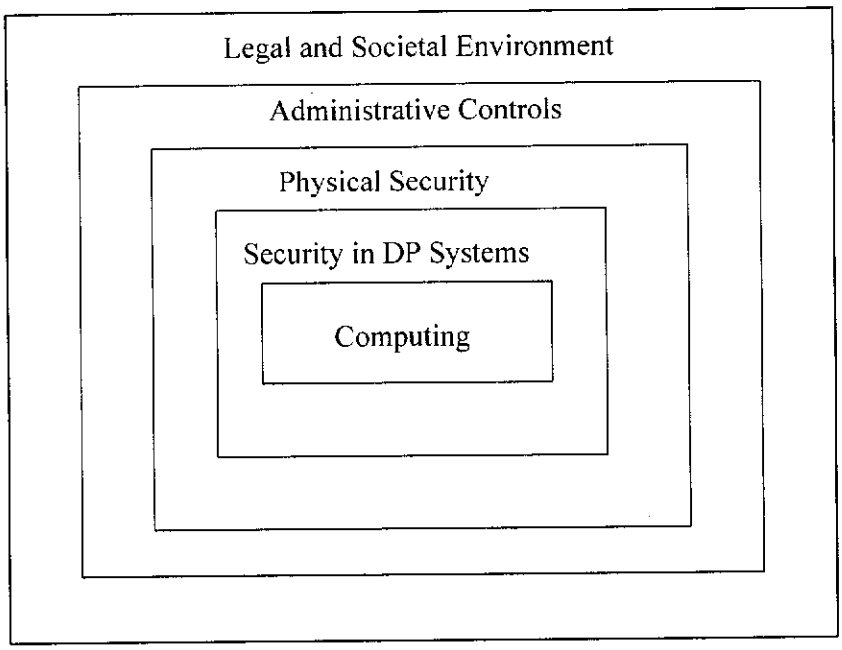

Figure 3.1: Onion Skin Model (Smith 1993, p56)

The onion skin models evolved as security became a more prominent consideration for information systems managers and, as is common with early model building, they have a number of shortcomings. One of the major problems with this type of model is the implication that each layer is isolated and quite separate in character and communication with other layers, hence no interaction takes place between the layers. In practice, however, the layers are inter-related and action in one layer may directly or indirectly affect other layers.

Many authors presenting onion skin models do not discuss the associated limitations, however Smith (1993) and Martin (1973) recognise such a simplistic representation may lead to incorrect assumptions. The layered model suggests "all security actions will have some effect against all possible threats, and that perfect protection of the system could be achieved by perfect implementation of any one of the layers of security" (Smith 1993, p55). Such an interpretation could lead to misguided management decisions resulting in under or over-protection of information assets.

Onion skin models are broad and simplistic representations of situational factors that may, or may not, affect security management. There is little detail of specific desired controls relating to either the information systems or the environments in which they operate. The organisational and technical factors are simplistic and general in nature and have limited coverage in these models. There appears to be no specific or general consideration of human and social factors.

With regard to strategic direction, there is no mention of organisational goals or links with strategies. This type of model displays a high level of abstraction with little definition of component characteristics or their interaction. The range of layers encourages proactive management but is limited in its ability to be applied in practice due to the generalised nature of its structure and content. The broad boundary afforded by the model attempts to give a holistic view of security however the integration of functions and controls is not addressed. Unfortunately, this model type does not encourage or address the inclusion of security as part of the organisational culture.

3.2.1.2 Checklist Models

Checklist models use comprehensive lists of threats or security actions organised under specific headings. This type of model is used mainly for security reviews and audits. It's purpose is to check the presence and operation of specific controls or the possible existence of threats. Checklist models are widespread and some examples can be found in Fisher (1984), Forcht (1994), Jackson (1986), Moeller (1989), Vasarhelyi and Lin (1988), Watne and Turney (1990) and Wood et al. (1987). Checklist models are usually extensive in range, attempting to cover all possible threats in all types of environment.

Although the comprehensiveness of the checklist contents is held to be one of this model's strengths, it is also seen to be a weakness. This type of model tends to specify all controls for every system, not just those appropriate to the particular system under inspection (Kiountouzis and Kokolakis 1996) and have been observed to be over-extensive in nature (Backhouse and Dhillon 1993). Checklists have also

been heralded to give incomplete consideration of the overall computer security environment (Carroll and MacIver 1984).

The application of checklist models is a straightforward exercise. The environment is checked for each control or threat listed and some indication of its existence is noted, for example, a tick or a low-medium-high rating. In practical application terms checklist models can be laborious and time-consuming to implement, with many of the factors listed being of minor importance to the environment under study. A further shortcoming of the checklist approach is the lack of depth involved in determining the existence of a listed security measure. This method does not encourage further investigation of the situation under study past those items included on the checklist.

A more sophisticated type of checklist model utilises methods concentrating on the economics and cost-justification of solutions (Earl 1989; Parker, Benson and Trainor 1988; Pfleeger 1997; Wolfe 1995). These approaches generally look at the value of assets and having calculated a potential dollar loss from given threats, then assign a savings element that is used for cost justification of a given countermeasure. Dhillon and Backhouse (1994b) suggest these models tend to impose a "tidy" structure on to risk assessment. Angell (1993, p385) believes this approach is limited because "the values of accountancy, in so-called information audits ... imply that all decisions can be reduced to a form of algorithmic bookkeeping".

As with onion skin models, checklist models concentrate on technical elements, particularly with relation to computer hardware and software, with only limited consideration of organisational factors. Social and human factors are not commonly included in the design or application of checklists and cost-justification methods.

The checklist approach is likened to a policing facility for regulating and controlling safeguards within the organisation. Unfortunately, the segmented nature of the list items under specific headings supports a piecemeal application of security within the organisation. There is no alliance of security list contents with organisational strategies and no endeavour to integrate security into the organisational culture. In

addition, the method does not attempt to raise awareness of security issues nor encourage ownership of protective measures by stakeholders.

3.2.1.3 Matrix Models

Matrix models of security feature simultaneous consideration of more than one aspect or dimension at a time. Matrix models are commonly built upon rectangular axes to enable the matching of horizontal and vertical elements and are often used in risk analysis models. For different types and applications of matrix models see Bhaskar (1993, p2), Fisher (1984, pp73, 93, 111, 131, 143), ISACA (1995), ISACF (1995), Krueger (1993), McCumber (1991) and Parker (1981, p56). Many of these matrix models are simplistic in nature and application. On the other hand, comprehensive, non-trivial multi-dimensional matrix models can give a much broader view of factors effecting the organisation's security. These models are thus able to illustrate component elements of each dimension and their links to other elements.

Matrices ideally contain mutually exclusive dimensions composed of mutually exclusive elements. This ensures there is no overlap between variables under consideration and aids validity of both quantitative and qualitative analysis performed on those variables. A well-designed matrix can provide a compact, cohesive, comprehensive and well-integrated tool to managers, for either qualitative or quantitative decision making.

The two matrix models cited above are of particular interest in this research - the McCumber (1991) model (see Figure 3.2) and the COBIT model (see Figure 3.3). The McCumber model matches three dimensions; information states, information characteristics and security measures. The three Information States are transmission, storage and processing. The Characteristics of information needed are availability, integrity and confidentiality. Security Measures implemented can relate to either technology, policy and practice, or education and training.

Each element of a particular dimension can be matched with any element of the other dimensions to give guidance for management decisions. McCumber suggests the model can be applied to IS development, IS auditing, and evaluation of IT security systems. In an auditing setting the critical characteristics of information (availability, integrity, confidentiality) are identified for each of the three information states (transmission, storage, processing) and security measures in practice are then reviewed under the areas of technology, policy and practice, and education and training.

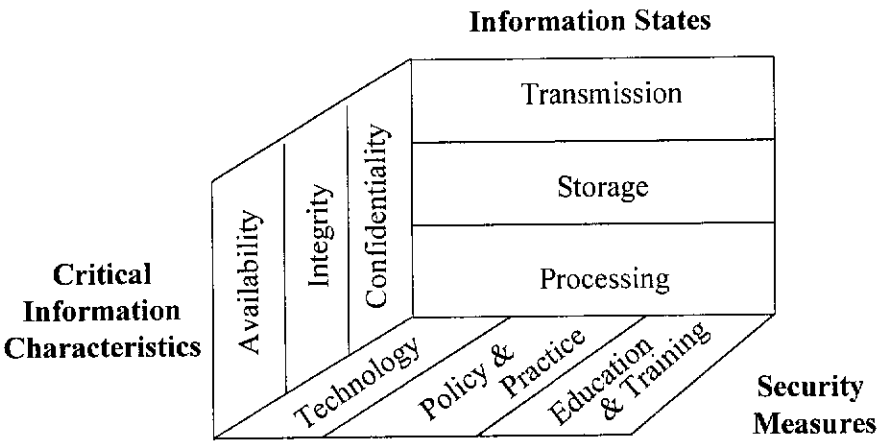

Figure 3.2: McCumber Matrix Model (Source: McCumber, 1991)

In an IS development environment security measures are included in a new system based upon the critical information characteristics applied to each information state. For example, encryption hardware and software (technological security measure) could result from the need for confidentiality (critical information characteristic) of information transmission (information state).

The application of the model into practice is not readily apparent to the untrained user. The complex and abstract nature of the factor linking process highlight the model's academic, rather than practical nature. However, the McCumber model is more extensive than previously discussed models in its coverage of factors affecting the safekeeping of organisational information. A wider view of organisational and

technical factors is given, but there is no recognition of human and social factors other than the need for education and training.

This model appears to be aimed at an operational level with no specific reference to strategic level goals. It can be used to indicate preventative security measures for given situations or areas within the organisation. The model attempts to present a more extensive and integrated view of organisational considerations for security than previously discussed model types. However, the format of a matrix does not engender natural flow or easy conversion into a broad, organisational perspective. There is no suggestion within the model that security considerations become part of the organisational mind-set in day-to-day management and operations, or the allocation of security responsibility to roles or areas.

The COBIT framework has been designed by the Information Systems Audit and Control Foundation as a set of IT control objectives. It is a tool designed for auditors and business managers to aid the development of clear policy and good practice for IT control. It is based upon the premise that "IT Resources need to be managed by a set of naturally grouped IT Processes to provide the information that the enterprise needs to achieve its objectives" (ISACF, 1995, p3).

The three dimensional model (see Figure 3.3) features the linking of IT Resources, IT Processes and Information Criteria. IT Resources include people, application systems, technology, facilities and data. IT Processes are defined at the lowest level into activities or tasks. Activities are then grouped into naturally occurring processes to form domains at the highest level. Information Criteria comprise quality requirements (quality, cost, delivery), fiduciary requirements (effectiveness and efficiency of operations, reliability of information, compliance with laws and regulations) and security requirements (confidentiality, integrity and availability). The matrix is designed to be approached from any one of the given dimensions.

The basic premise of COBIT is "control in IT is approached by looking at information that is needed to support the business processes and by looking at information as being the result of the combined application of Information

Technology related resources that need to be managed by IT processes" (ISACF 1995, p7).

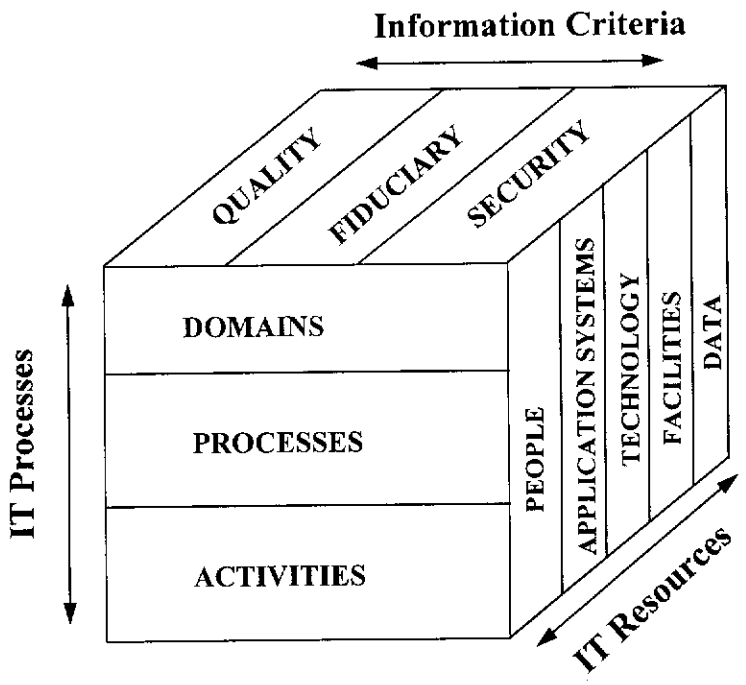

Figure 3.3: COBIT Framework Source: ISAC, 1995, p11

In order to achieve this the model contains four domains; planning and organisation, acquisition and implementation, delivery and support, and monitoring. The planning and organisation domain centres upon the contribution of information technology to the achievement of business objectives, and the development of an appropriate technological infrastructure. The acquisition and implementation domain identifies IT solutions and integrates these into business processes. Delivery and support is concerned with the ongoing support of the solutions and includes operations, security, continuity and training. The monitoring domain centres upon regular assessment of quality and compliance to control requirements.

The full COBIT model is still under development. The first phase was the production of the framework illustrated in Figure 3.3, and its linking to current international audit control objectives and guidelines. The second phase will provide

an automated version of the model and provide self-assessment guidelines for IT managers. The final phase will consist of performance indicators and the addition of further control guidelines and audit objectives. The framework presented to date far surpasses any previously discussed model in depth and sophistication of content. The structure of the model is highly complex and will need a software product to aid its application into a business organisation.

The COBIT framework includes technology as part of the IT Resources dimension encompassing hardware, systems software, database management systems, networking, multimedia and the like. The wider consideration of organisational factors such as organisational goals, planning and business practices gives a deeper appreciation of the organisation as a whole and the interrelationship of its components. The recognition of people as an element of IT Resources includes consideration of skills, awareness and productivity factors, thus more fully appreciating the human element within IT systems. There needs to be a more significant role of education and training within the model, particularly with regard to information security (Yngstrom 1996). It is currently unclear where education and training fits into the model apart from within the delivery and support function, relating to the ongoing operation of IT solutions.

Social aspects are addressed only in relation to the integration of people with other IT Resources, IT Processes and Information Criteria. The framework incorporates strategic goals and business objectives within the planning and organisation domain of IT Processes, and as the model stands this theoretically links with security as an Information Criteria. COBIT's consideration of an extended set of elements encourages a holistic view of security, however, the inclusion of security into organisational culture is not specifically addressed.

It is not clear from the model or the navigation aids provided how the dimensions are linked and this will be important for decision makers using the model for guidance. The researcher has devised a table of dimensions and elements of the COBIT matrix to illustrate the non-conformity of its composition (see Figure 3.4).

IT Processes	IT Resources	Information Criteria
Domains - Planning & Organisation - Acquisition & Implementation - Delivery & Support - Monitoring	**People** - Skills - Awareness - Productivity	**Quality** - Quality - Cost - Delivery
Processes for Planning & Organisation Domain - Define a Strategic Plan - Define Information Architecture - Determine Technological Direction - Define Organisation and Relationships - Manage the Investment - Communicate Management Aims and Direction - Manage Human Resources - Compliance with External Requirements - Assess Risks - Manage Projects - Manage Quality	**Application Systems** Sum of Manual and Programmed Procedures	**Fiduciary** - Effectiveness & Efficiency of Operations - Reliability of Information - Compliance with Laws & Regulations
Processes for Acquisition & Implementation Domain - Identify Automated Solutions - Acquire and Maintain Application Software - Acquire and Maintain Technology Infrastructure - Develop and Maintain Procedures - Install and Accredit Systems - Manage Changes	**Technology** - Hardware - Operating Systems - Database Management Systems - Networking - Multimedia	**Security** - Confidentiality - Integrity - Availability
Processes for Delivery & Support Domain - Define Serve Levels - Manage Third Party Services - Manage Performance and Capacity - Ensure Continuous Service - Ensure Systems Security - Identify and Attribute Costs - Educate and Train Users - Assist and Advise Customers - Manage the Configuration - Manage Problems and Incidents - Manage Data - Manage Facilities - Manage Operations	**Facilities** Resources to House and Support Information Systems	
Processes for Monitoring Domain - Monitor the Process - Obtain Independent Assurance	**Data** Data Objects, ie External and Internal, Structured and Non-structured	
Activities (not defined)		

Figure 3.4: Elements of the COBIT Framework Dimensions

As this table illustrates, the IT Processes dimension is a hierarchical set of elements, with each level in turn exploding into a subset of lower level elements, i.e. Domains break down into Processes which are composed of Activities. Hence Domains, Processes and Activities are not mutually exclusive elements of the IT Processes dimension, and are only abstract classification labels for the contents of that dimension.

The two remaining dimensions, Information Criteria and IT Resources, are composite dimensions, with each element representing a mutually exclusive variable characterised by specific features or criteria which may or may not be measurable. For example, Security is a mutually exclusive variable of Information Criteria, characterised by integrity, availability and confidentiality; and People is a mutually exclusive variable of IT Resources, characterised by skills, awareness and productivity indicators.

In order for the COBIT matrix to be truly three dimensional with mutually exclusive elements, the IT Processes dimension should be comprised of four elements: planning and organisation, acquisition and implementation, delivery and support, and monitoring. These elements are currently presented as the Domains of IT Processes. In explanation of the IT Processes domains, ISACF (1995, p10) states "the principle applied is that the IT Resources need to be managed by a set of naturally-grouped processes, in order to provide the information that the enterprise needs to achieve its objectives". The diagram shown in Figure 3.5 offered by ISACF attempts to illustrate this concept.

The lower circle of the diagram consists of elements labelled Planning & Organisation, Acquisition & Implementation, Delivery & Support and Monitoring, representing the domains of the IT Processes dimension. These domains are linked to the higher circle by the IT Resources dimension. The higher circle consists of elements labelled Business Processes, COBIT, Information and IT Resources, with a set of Criteria appearing in the centre of the circle.

These criteria appear to relate to the dimension Information Criteria although this is not explicit by the positioning of the criteria box in the diagram. It is unclear from this diagram how Business Processes and COBIT relate to the three dimensions of the COBIT framework.

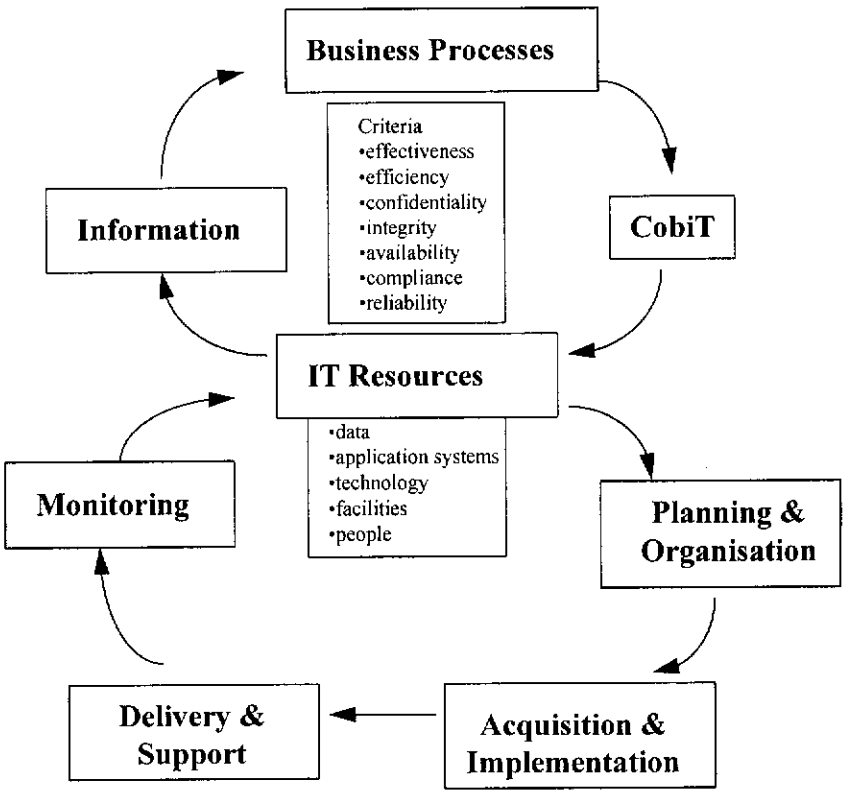

Figure 3.5: The Application of COBIT : source ISACF, 1995, p11

It would appear that the dimensions of the model are illustrated in a non-consistent manner. The linkage between the elements in the higher circle is not discussed, nor is readily apparent. The inclusion of the COBIT element in the higher circle is confusing, as COBIT is used to refer to the complete framework, consisting of the three dimensions, IT Processes, IT Resources and Information Criteria.

There is also no explanation of the Businesses Processes element at the top of the higher circle, or how this relates to the other elements, particularly the COBIT and Information elements with which it has direct flows. One final observation is the

absence of enterprise objectives in the model, and the linking of organisational objectives is claimed to be a key feature of the COBIT approach.

Overall, the COBIT model offers the information security manager and IS auditor a comprehensive tool for analysis of security needs. It would appear, however, that the lack of clarity evident in the model and the lack of navigation aids for application limit its ability to be applied without some confusion.

Risk analysis is one of the most common uses of matrix models, particularly addressing the threats of intrusion, virus infection, unauthorised access and system malfunction or non-operation. (See, for example, Anderson, Longley & Tickle 1993; Clark 1989; Ekenberg, Oberoi & Orci 1994; Fletcher 1994; Mostert and von Solms 1993; Orlandi 1986.) This group of studies "has been closely associated with computer scientists who are concerned with providing ever so complex technological solutions" (Dhillon and Backhouse 1994b, p2). Matrix and checklist models used in risk analysis are incomplete in their consideration of the system at hand and their probability estimates have a questionable relation to reality (Baskerville 1988). "Risk arithmetic can become unrealistic with low probabilities modifying enormous losses. The monetary basis of risk analysis is unable to legitimately address the social importance of safety, privacy and accuracy." Baskerville (1988, p85).

Risk management approaches assume all risks can be transformed into tangible and definitive numeric values. To achieve a meaningful result, accurate estimates must be made regarding potential losses and rates of occurrence, and intangible factors need to be converted into a tangible form in order to be quantified. Parker (1991) believes that the whole question of security should be centred upon a standard of due care (avoiding negligence) in achieving security rather than measuring security by risk of loss.

3.2.1.4 Filter Models

Filter models encompass tables (simple two-dimensional matrices) and sequential flow models. Activities and influencing factors filter from one stage or criteria to

another. The majority of filter models are simplistic in nature, having only one or two dimensions. The Idealised Development Path model for information security is illustrated in Figure 3.6 (Jackson and Hruska, 1992). In this model, the management of information security can be approached from either a formal or informal standpoint. The starting point for both the formal and informal paths is the security policy, for without the policy the security to be implemented is not known.

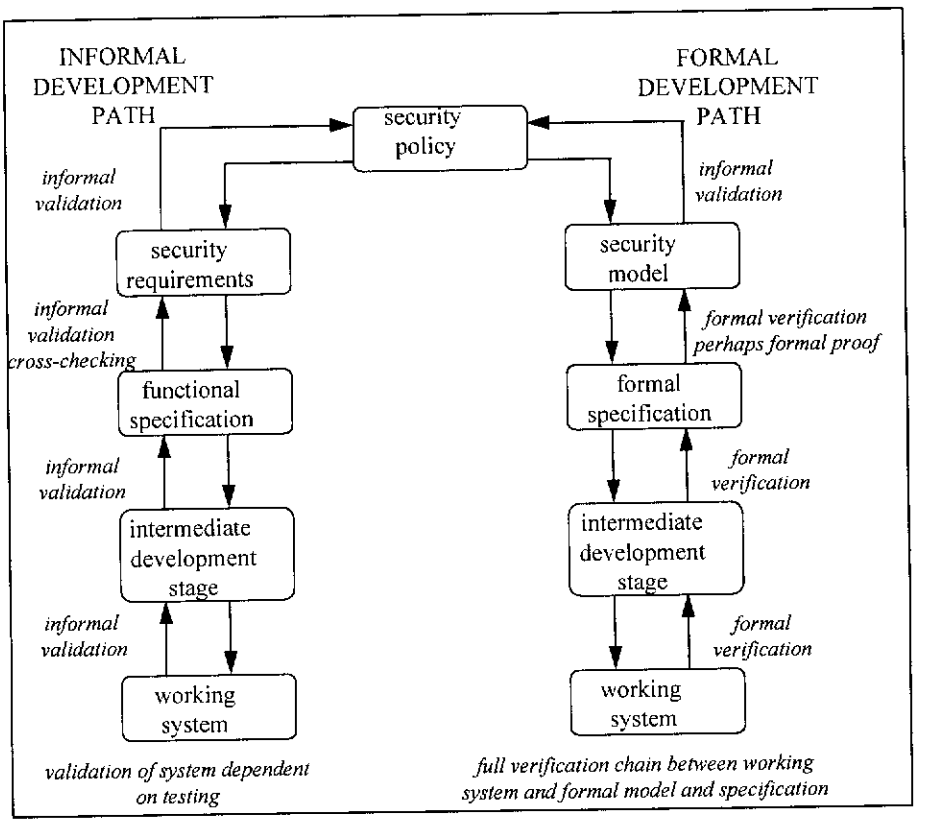

Figure 3.6: Idealised Development Path Model

Source: Jackson and Hruska, 1992, p199

The informal approach uses information from the security policy to specify requirements for identification and authentication, access control, accountability, auditing, availability and assurance. The functional specifications are a definitive description of what the system will do based upon the requirements, concentrating on assuring completeness and correctness. These functional specifications are then used to build and implement the system. Testing is the key to ensure validation, i.e. that

the system built is an accurate and complete implementation of the system defined by the functional specifications.

The security policy is then used as a basis for the development of the security model. The security model is not a set of requirements, but an abstract set of rules by which the security policy is to be upheld. The final working system must be continually verified by mathematical testing through the progressive stages of development.

This model does not include considerations of organisational objectives or how these influence the building of the security policy. It concentrates on technical aspects of fulfilling requirements and specifications with no inclusion of human or social factors. There is little discussion regarding practical application of the model except that the formal approach is used by US Government and Defence organisations. Due to the narrow perspective offered this model appears to be limited in its applicability.

The filter model described by Smith (1993) is less sequential in nature, matching threat conditions with security actions. One of the important features of the model is the minimisation of overlap of elements, which is important in the design of the basic model and subsequent quantitative analysis carried out on the elements. Security actions are categorised into operating environment, access controls, personnel, routine operations and selection and review. Threat categories comprise environmental problems, system error, operator error, fraud, espionage, vandalism and theft. The relationship between actions and threats is illustrated by way of a matrix (see Figure 3.7) and rated at either Nil, Low or High. The ratings contained in the model have been developed based upon the analysis of numerous other security models and research.

A Nil rating indicates that the action will have no significant effect on security in relation to that particular threat. A Low rating indicates there is a significant relationship hypothesised, but the effect of the action will be small in impact on that threat. A High rating indicates a significant relationship of high impact between the action category and the level of security against the threat type.

	Environ-mental Problems	System Error	Operator Error	Fraud	Espionage	Vandalism	Theft
Operating Environment	High	Low	Nil	Nil	Nil	Low	Nil
Access Controls	Nil	Nil	Low	High	High	High	High
Personnel	Nil	Nil	High	High	High	Low	Low
Routine Operations	Low	Low	High	High	Low	Low	Low
Selection & Review	Low	High	Low	High	Low	Low	Low

Figure 3.7: Filter Model of Threats and Security Actions

Source: Smith 1993, p61

The central hypothesis is that the effect of each security action is selective and will not impact all threats. The filter model may be likened to the effect of coloured filters on light. Each filter removes some hues and leaves others untouched, and additional filters will have little effect on the resultant colour of the emergent light if those colours have been removed by the effect of previous filters. So the effect of new security action may be minimised where threats have been countered by other actions.

This model is a useful illustration of the link between security actions and threats in given situations. However, it can only be applied to a specialised area of IT operations, and does not offer a holistic view of security for an entire organisation. The model itself contains little account of organisational and social factors. The technical and people factors are limited to those threats and security actions relating directly to technology and people within a specialised IT area. The application of the model encourages a recognition of necessary security actions for given threats and acknowledgement of the effects of security actions upon those threats. However, there is no link with business objectives or organisational goals, and the model does not address the embedding of security considerations into the organisational mindset.

3.2.1.5 Socio-Technical Models

Socio-technical models define preventative security and are characterised by the inclusion of human and social factors in addition to technical considerations. Examples of socio-technical models include the IBAG Framework (Clark 1993; Sundt 1994), the Parkin model (Parkin 1993), the Wilson model (Wilson, Turban & Zviran 1992), The Common Denominator (European Security Forum 1995b) and the SBC Model (Kowalski 1994).

The SBC model uses a layered framework of Social and Technical measures (see Figure 3.8), and the aim of the model is to present an abstract thinking aid to management (Kowalski 1994). Social security measures are layered into ethical-cultural, legal-contractual, administrative-managerial-policy and operational-procedural sections. The Technical measures are classified into mechanical-electronic and information-data layers.

The first layer of the social classification is ethical-cultural measures, these being defined as "educational and informative measures taken to clarify particular ethical and cultural problems relating to the use of IT within the organisation" (Kowalski 1994, p237). These include codes of ethics, brochures or memorandums, seminars, conferences and training programs.

Legal and contractual factors involve the production of evidence to be used by criminal investigators in an IT criminal trial determined by the procedural laws imposed by the IT system owner and law enforcement resources available. Administrative and managerial prevention measures include management activities focused on the monitoring and control of personnel, with administrative measures concentrating on formulation and control of IT security policies and regulations. Operational and procedural measures are the conversion of goals and policies into concrete activities.

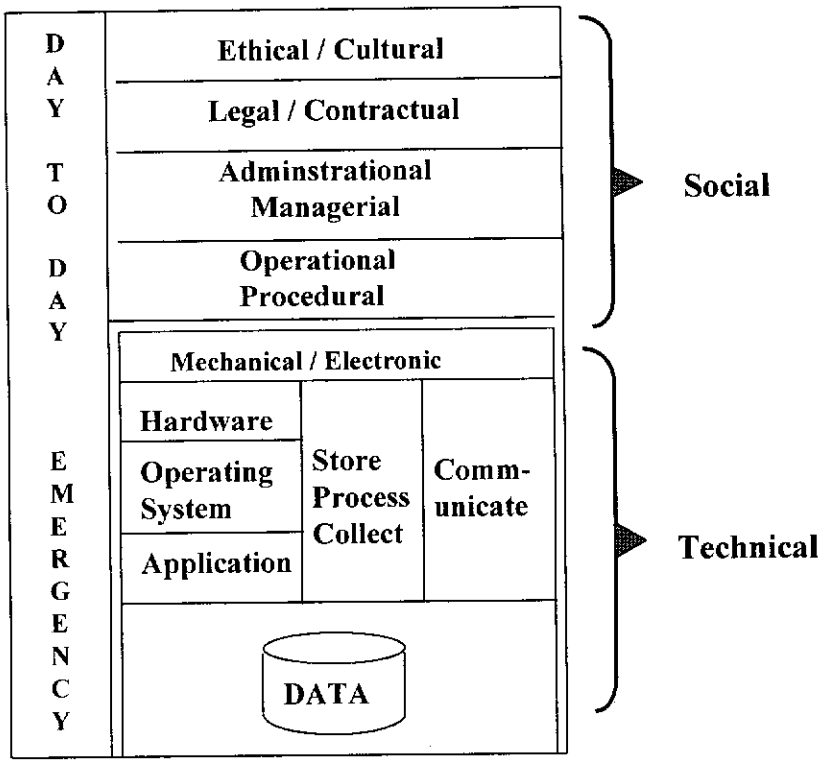

Figure 3.8: SBC Socio-Technical Model

Source: Kowalski 1994, p19

The abstract nature of each set of factors is related to its position in the model. For example, ethical measures are more abstract (and less concrete) than legal controls, which are more abstract than policy measures, which in turn are more abstract than procedures, with procedures being the most concrete type of social IT control measure used within the organisation.

The Technical set of IT control measures include those which relate directly to the technology in machine form or the software and processes involved in its operations. Security measures covered by the mechanical and electronic layer centre around restricting physical access to IT systems. Computer hardware measures include protection mechanisms such as tamper-resistant modules, multi-state machines, fault tolerant circuits and encryption devices. Operating System protection includes measures such as security kernels, discretionary or mandatory access control and off line and real time auditing. Controls included in the Application layer are integrity and consistency controls in software, roll-back facilities in database systems and

concurrent auditing functions in distributed applications. Although these layers are hierarchical, the non-hierarchical functions of collecting, storing, processing and communicating information are applied to all layers with the technical section.

There is often an inconsistency between day-to-day and emergency protection mechanisms implemented within an organisation (Kowalski 1994). For example, an IT system may be protected against terrorist bomb attacks, but not protected against users spilling coffee on a disk station. Day-to-day and emergency security measures should thus be applied across all layers of the model.

The model can be applied at an international, national or organisational level. It has been applied in a number of IT security situations, including IT systems communications (Kowalski 1994), IT crime prevention (Kowalski 1993), comparing national computer security policies (Kowalski 1991a) and a mental model for IT security (Kowalski 1991b).

This model certainly addresses social considerations in its ethical and cultural, legal and contractual layers, with the emphasis being on social factors within the given scope, i.e. nation, organisation, etc. The human element is recognised in part through the ethical and cultural layer, however, there is no discussion of the involvement of personnel in the planning or managing of security or assignment of security responsibility. Technical aspects of security are adequately addressed in the technical section of the SBC model ranging from the pure technology to the mechanisms supporting that technology.

The alliance of security with organisational goals and strategy has not been addressed in the SBC model. However, a proactive management approach and a holistic view of security are encouraged. The inclusion of security into the organisational culture is not specifically encouraged in the model.

Another example of a socio-technical model is the Virtual Methodology (Hitchings, 1995), which claims to incorporate technical, organisational, contextual and human issues into the study of information systems security. The Virtual Methodology is "a

framework that can be adapted by organisations in order to reveal the major information security issues of the organisation" (Hitchings 1995, p369). Its aim is "to assist in developing security at an adequate level for a particular information system" (Hitchings 1995, p371). The Virtual Methodology consists of seven phases; analyse the organisation, analyse the system in context, analyse the system and determine risk areas, analyse the system and determine types of controls required, design controls, implement the system and review, and maintain the system (see Figure 3.9).

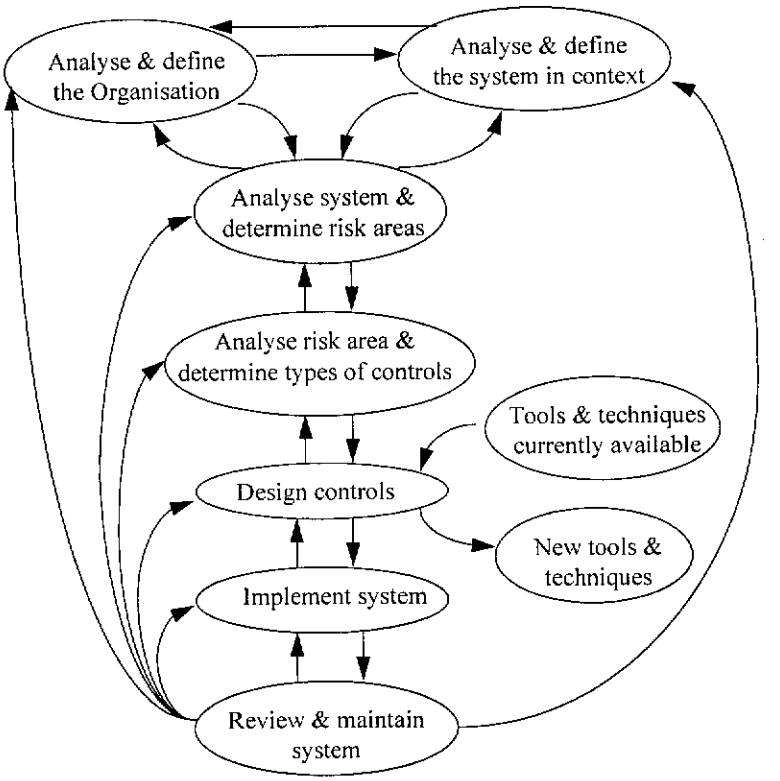

Figure 3.9: Virtual Methodology Phases
Source Hitchings 1995, p372

The first phase develops a model of the organisation describing the structure and philosophy of the enterprise and its functions. Phase two involves analysing the information systems under study in context, producing an information systems model showing interactions. The third phase utilises the models from the previous two phases to create a model of risk areas. These risk areas are analysed in the next phase

to determine the types of controls needed. During phase five controls are designed for each risk area identified, and associated costs and benefits considered. The controls are implemented in phase six, with the final phase consisting of a review and maintenance function. The first four phases are conceptual rather than physical phases, as alterations can be more easily applied at a conceptual level than within a physical implementation.

Given organisational factors are designed to be covered in the modelling of the organisation phase. A consideration missing from the model is acknowledgment or seeking out of organisational objectives and the methodology does not appear to analyse the role of security in achieving those goals. The human element is recognised and users are encouraged to participate. However, the assignment of security responsibility is not included, and at no stage is security training or awareness education recommended. The methodology is not clear in its coverage of technical factors, both of the technology itself or its supporting mechanisms. Social factors are acknowledged in the analysis of employee-to-employee and employee-to-outsider transactions.

There is no recognition of organisational missions or goals and how security integrates with organisational strategy. There is also no encouragement to build security into the organisational culture. The methodology does review the current situation to identify risks and encourages proactive security management only at a system level. Because the model is focussed purely on the security of a single information system the methodology does not support an holistic view. Solutions are designed for a given system with limited analysis of the effects on other systems or security measures. It would appear from the discussion of application of the methodology (Hitchings 1996) that this approach encourages piecemeal solutions designed for independently studied risks within a single and isolated information system.

3.3 DISCUSSION

The above analysis of current information security management models results in the following findings:

1. All models offer guidance relating to desired security measures forming the protective boundary around information and information-related assets.
2. The majority of models encourage or can be used to provide a proactive approach to managing security, supporting preventative action rather than reaction to security violations.
3. Very few of the models acknowledge the role of security in achieving organisational goals and missions.
4. None of the models encourage users of the information and systems to take responsibility for security, or assign roles and responsibilities for security measures in operations.
5. Very few models encourage a holistic view of security with the majority focussed upon a single risk, security measure or information systems level.
6. Most acknowledge the need for user involvement, but few design processes to apply the model with high user interaction in planning and management of security, hence paying only lip-service to users and stakeholders.
7. Very few models recognise the need to raise the awareness of security and include security education and training in preventative management.
8. The majority of models concentrate on filling security holes in current systems and situation rather than seeing out innovative, integrated means of minimising risks.

Independent analyses of information systems security models has discovered the static, categorical and typological nature of ring, checklist and matrix models in particular, the majority being conceptual and passive (Baskerville 1988). These models are referred to as *iconic* models and "it is assumed that all information systems will exhibit the same or very similar traits and behaviour" (Baskerville 1988, p111). The information security industry needs a more dynamic and fluid model, one that is able to be applied to a variety of different systems. This is illustrated by

Harre's (1972) differentiation between *homeomorphic* and *paramorphic* models. Homeomorphic security models assume that the source model and the subject model are identical. The application of the source to the subject prescribes needed features or identifies missing security measures or features, whether or not these are applicable to the situation in hand. On the other hand, paramorphic security models assume the source and subject models are different, thus enabling such aspects as mission and environment to influence the recommendations. This suggests a dynamic paramorphic security model could be more suitable than the homeomorphic models of the past, particularly one that considers the identification of risk vectors (sources from which risks emanate) and targets towards which those risks are directed (Baskerville 1988, p112).

Other problems identified with current approaches include the use of technical "kludges" to solve business issues, the non-acceptance of responsibility by information owners and users, and the lack of end-user involvement in the security management of their own information (Firth 1993). Traditional approaches do not appear to be working for a variety of reasons, including inflexible or rigid structure, lack of user involvement, lack of management participation and support, academic and theoretical character, difficulty in applying in practice, or based upon scientific methods that are not appropriate to human related systems environments (James, Andronis & Paul 1996).

One of the major concerns related to the traditional approaches is the insignificant role of people and 'people' considerations. Information systems are human-related systems: humans design and develop the hardware and software; humans operate the computer systems controlling the organisation's corporate information database, and humans use the computers and information in their areas of work. Information security is not primarily a technological concern as also includes psychological and sociological behaviour of people (Parker 1981). It is the human element in the information systems equation that is the key to effective information security management. The actions and attitudes of people directly affect security, as computers are not themselves capable of abuse and misuse.

According to Angell (1993, p382) the traditional approaches are superficial because their view focuses on technical installations and on their functionality, "information systems are complex socio-technical systems, which impact on the well being, on the integrity of the whole organisation." The importance of the human element is also illustrated by the unique nature of people compared to machines. "The notion of security is not merely a question of machine-machine relations, but complicated by the complexities, (inter) dependencies and frequencies of human-machine relations. The human dimensions are crucial, because of the essentially pragmatic nature of all information and the human struggle for competitive advantage and ultimate survival affecting trust and confidence. In contrast, machine breakdowns can be calculated" (Will 1992, p18).

The use of highly scientific and homeomorphic approaches to IS security concentrating on technological issues has been the dominating approach for a number of decades. The premise that information systems are developed by *people,* for use by *people* to enable them to accomplish tasks to assist individuals and organisations in achieving their goals, appears to have been forgotten. As the implementation of technology merges more markedly with organisational practices and strategies, so information systems security must be managed actively and with purpose. The past technical and complex methods of security assessment provide a partial answer to effective security management. However, more consideration needs to be given to the human and organisational elements to raise the profile of information security and make protective measures more appropriate to the corporate environment. Hence it seems that the highly inflexible and complex technical traditional approaches to planning and managing information systems security are inappropriate in the current changing technological and organisational environment.

The need for a wider view of information security within the organisation has been visited in Chapter 2. A necessary part of any security management approach is the analysis of risks imposed by intentional and unintentional threats via acts of God, human error and abusive acts. To analyse risks comprehensively it is necessary to not only identify such risks but also recognise the associated vulnerabilities and assess exposure levels. Management must understand the nature of the threat and the

vulnerability that threat creates in order to effectively manage any associated exposure. Without an awareness of risks and a dedication to uphold security controls already in place, none of the traditional methods are likely to succeed. There is a need for more involvement of stakeholders in the planning and ongoing management of information security.

3.4 CHAPTER CONCLUSION

Although currently available information security management models support a preventative and proactive strategy the majority are complex in design and not pragmatic in nature. User involvement levels are low, there is little or no alignment of security with organisational goals, and solutions are based upon isolated areas of identified vulnerability. Approaches considering human, organisational and social factors in addition to technical concerns are only just beginning to emerge.

The shortcomings of current approaches to the management of information security reinforce the need for a more encompassing model or approach. Such an approach would incorporate factors relating to the technology, as well as organisational, human and social factors influencing the security of information assets. An aim of this method would be to raise awareness of security issues at all levels and encourage employees to take responsibility for security issues within their own work areas. To achieve this aim it is desirable to involve employees in the planning and management functions surrounding security.

As one solution, Checkland's (1981) Soft Systems Methodology (SSM) has been suggested a forerunner to a risk analysis approach in order to incorporate more human factors into a predominantly physical process (Lane 1985). Unfortunately, the application of SSM before the risk analysis would still result in primarily physical solutions to security problems (Baskerville 1988). However, the combination of the two would raise the awareness of users and achieve a higher user involvement in the entire security management process.

4. RESEARCH METHODOLOGY AND DESIGN

4.1 CHAPTER INTRODUCTION

A research design is a technical plan that should assure the evidence to be collected is pertinent to the questions of the study and the approach covers competing concerns of the study (Yin 1989). Matching the research design with an appropriate research methodology is an important consideration in any research project. The methodology must not only be appropriate to the type of research, but also to the environment in which the research is being undertaken. This chapter discusses both qualitative and quantitative approaches, as both are used at different stages in this research. Methods used in information systems research and the specific methods applied in the study at hand are also discussed.

4.2 QUALITATIVE AND QUANTITATIVE RESEARCH METHODS

In choosing the type of research approach appropriate to any study it is necessary to consider the characteristics and aims of the two schools of research thought - positivism and interpretivism.

Positivism is based upon reductionist thinking, having its origins in the natural sciences and study of the laws of nature. Positivism uses quantitative measurement and replicable testing in its aim for generalisability and prediction. This traditional approach has been termed *nomothetic* by Franz and Robey (1984) and Weick (1984). Nomothetic research strategies are explained as methods seeking general laws and drawing solely on procedures used in the exact sciences (Benbasat, Goldstein and Mead 1987). In this style of research, a "hard" boundary clearly defining the system under study, separates the researcher from the system being researched (Perry and Zuber-Skerritt 1991), aiming for total objectivity. Using reductionist thinking, the system is decomposed into parts and (usually) quantitative analysis applied to a small number of variables, assuming all other system variables are held constant. This type of research appears to be particularly appropriate in the natural sciences.

Interpretivism, on the other hand, is based upon a relativistic view of the world having its main application in the social sciences. Interpretivism uses qualitative methods to seek out explanations and gain an understanding of human and social systems. Perry and Zuber-Skerritt (1991) suggest these systems are "soft" systems without clearly defined boundaries between the researcher and the system of which the researcher is unavoidably a part. Interpretivism explores complex and dynamic issues relating to relationships between people and their physical and socio-cultural environments. This doctorate research is interpretivistic, investigating the improvement of information security management through the involvement of people in the planning process.

Whereas positivism is described by McCouat and Peile (1995) as having the goal of achieving universal laws about reality which provide a basis for predictive control, interpretivism opposes the search for universal theories, believing knowledge is not about control . Intepretivists seek to understand the meanings and interpretations people have about their own experience and recognise that these meanings are socially constructed (McCouat and Peile 1995). One of the essences of qualitative research is the study of elements in their natural environment (Darke, Shanks and Braodbent 1998; Silverman 1998). Denzin and Lincoln (1994) believe an important element is that qualitative reseachers attempt to interpret phenomena in terms of the meanings people in the given situation bring to them. Qualitative research is referred to as illuminative research, where illumination comes from systematic integration of experience and whatever subjective data can be gathered, with the aim of making the best decision under conditions of limited time and resources (Standen 1995).

There has been much debate regarding the inappropriateness of quantitative approaches to research in the social sciences. For example, 'once one relaxes the ontological assumption that the world is a concrete structure, and admits that human beings, far from merely responding to the social world, may actively contribute to its creation, the dominant methods become increasingly unsatisfactory, and indeed, inappropriate.' (Morgan and Smircich 1980, p498). Interestingly, McCouat and Peile (1995) suggest that the qualitative and quantitative within positivism and

interpretivism are inseparable as each relies on the other for definition; ie, each defining its objectives and characteristics in opposition to the other.

To further this view, Standen (1995) believes that research, whether quantitative or qualitative, is an activity more valued for its help in problem solving than in arriving at generalisable conclusions meeting external standards of rigour. Morgan and Smircich (1980) highlight the link between theory and method when considering choice of a research methodology; this link being between the world view to which the researcher subscribes, the type of research question posed, and the technique to be adopted as a basis for research. From the researcher's understanding of the literature it appears each method has its most preferred application, and the research environment and character of the study at hand will be major considerations in choice of a qualitative or quantitative research approach.

4.2.1 Shortcomings of Qualitative Methods

Qualitative research methods have their shortcomings and the main criticisms levelled at qualitative approaches include:

- Validity is questionable due to the lack of rigour (Jarvenpaa, Dickson and DeSanctis 1985; Dick 1992 and 1993)
- Reliability is questionable (Jarvenpaa, Dickson and DeSanctis 1985; Henderson 1995), as data collection methods (commonly interviews and observations) are perceived to be fraught with bias. The data collected via these methods is more subjective than objective and Henderson suggests such data could imply opinion rather than fact, intuition rather than logic and impression rather than confirmation.
- Researchers lack clearly defined criteria for drawing meaning from qualitative research results (Miles and Huberman 1984)

In qualitative research Henderson (1995) suggests validity refers to gaining knowledge and understanding of the true nature, essence, meaning, attributes and characteristics of a particular phenomenon. Measurement is not the aim but rather

the knowing and understanding. Although numerical data can help to predict cause and effect in phenomena it does not necessarily bring out the richness of data from the perspective of the informant. Because quantitative studies are restricted to readily measured static constraints, they neglect aspects of the cultural environment, and social interaction and negotiation which Lyytinen (1987) believes could affect the outcomes. Kaplan and Duchon (1987) suggest these aspects also affect the constructs under study, in addition to attempting to avoid prior commitment to theoretical constructs or to hypotheses formulated before gathering any data.

Dick (1992 and 1993) believes qualitative methods should be used where the research problem situation is "fuzzy", (commonly a characteristic of social situations), as qualitative research can be more responsive to the situation. Although qualitative methods provide less explanation of variance in statistical terms than quantitative methods, qualitative methods can generate data forming the basis of new theories (Marcus and Robey 1988). This includes richer explanations of *how* and *why* processes and outcomes occur and related theories can be developed.

According to Henderson (1995) qualitative research rests on the assumption that human experiences and situations are unique and not necessarily accessible to validation via the senses. Qualitative researchers make no attempt to create and control conditions lending themselves to repeatability of the findings as variation rather than identical repetition is sought. "The purpose of qualitative research is to explore, describe, conceptualise and theorise about human experience in the natural setting. The aim is to go for fit between what actually occurs in the natural setting rather than replication." (Henderson 1995, p4).

Henderson goes on to suggest that in qualitative research the truth often lies in human experiences as they are lived and perceived by the informants rather than in the verification of priori conceptions of experiences, hence the quest for internal validity via testing and instrumentation appears to be inappropriate. In addition, the threat to external validity is actually minimised because the study is conducted in the natural setting and with few controlled conditions. This is because the informant's

experience represents a section from the real world, assuming it is well described (Henderson 1995).

Specific methods to ensure the validity and reliability of qualitative research have been suggested by a number of authors from different disciplines and include:

- Triangulation of methods (Dick 1992 and 1993; Eisenhardt 1989; Jick 1979; Standen 1995)
- Use of multiple observers or researchers (Dick 1992 and 1993; Eisenhardt 1989; Henderson 1995; Sandelowski 1986; Standen 1995)
- Deliberately attempting to disprove conclusions derived from the data, that is searching for negative cases, (Dick 1993; Sandelowski 1986)
- Cross checking data within and across cases (Eisenhardt 1989; Sandelowski 1986)
- Careful analysis of transcripts, logs or recordings (Standen, 1995)
- Use of standard classification systems (Standen 1995; Straub and Carlson 1989)
- Findings well grounded in the life experiences of the people studied encompassing both the typical and atypical elements, presented in a manner that people having the experience will readily recognise it as their own (Henderson 1995; Sandelowski 1986).
- Obtaining validation from the informants themselves (Henderson 1995; Sandelowski 1986).
- Prolonged contact with the informants (Henderson 1995; Sandelowski 1986).
- Theoretical sampling and independent analysis of data by other researchers (Henderson, 1995; Sandelowski, 1986).

Standen (1995) recommends that although research without rigour is inappropriate, to emphasise rigour over useability is to miss the point of qualitative research.

4.3 COMBINING QUALITATIVE AND QUANTITATIVE APPROACHES

Due to the diametrical opposition of qualitative and quantitative approaches, some authors believe the two methods cannot be mixed (McCouat and Peile 1995; Rodwell

1990; Peile 1994). Because information systems originated from computer science Fitzgerald, Hirschheim, Mumford and Wood-Harper (1985, p5) state that 'scientific proof is the only valid method and anything else is, at best, humourously tolerated as a form of quackery and, at worst, rejected out of hand. This viewpoint rejects the possibility that the combination of two or more alternative research approaches might lead to progress'. They go on to say that techniques used for data collection and analysis within the scientific method are not adequate on their own in areas involving human activity.

In the objective world of science, according to Drinan (1991, p93) there are plenty of dogmas and it has often been the case that breakthroughs have occurred only after the scientists have fundamentally changed their intellectual standpoints. This suggests the value of qualitative and action based research as a partner with the traditional scientific research approach, and 'the value of setting the global alongside the linear.'

Eisenhardt (1989) discusses the synergistic nature of a combination of both types of approaches. She believes that quantitative evidence can assist in three ways; firstly to indicate relationships which may not be conspicuous to the researcher; secondly, it can ensure researchers are not carried away by vivid, but false, impressions in qualitative data, and finally, it can promote findings when it corroborates those findings from qualitative evidence. Eisenhardt further believes that qualitative data, on the other hand, are useful for understanding the rationale or theory underlying relationships apparent from the quantitative data or may suggest theories that can be strengthened by quantitative methods.

A blending of qualitative and quantitative methods appears to have been used successfully in a number of reported research situations. A combination of methods is offered in Lee's Scientific Method, utilising both case studies and natural science quantitative methods (Lee 1989). Professional practice presents issues of such complexity that Wood (1995) calls for both qualitative and quantitative research methods, and applies a joint approach to research in a medical environment. Straub and Carlson (1989) also support the use of both approaches in IS research and highlight the need for valid and pre-tested research instruments. Their application of

combined methods is illustrated in publications reporting results of several research projects into IS security (see Straub and Carlson 1989; Straub and Hoffer 1988; Straub and Nance 1990; Straub and Widon 1984).

Further, Kaplan and Duchon (1988) discuss the success of combining qualitative and quantitative methods in other fields. They suggest such a combination provides a richer contextual basis for interpetting and validating results, introducing both testability and context into the research. In addition, using multiple methods increases the robustness of results as the findings can be strengthened by cross-validation. Kaplan and Duchon put their suggestions into practice using open-ended interviewing, observation, participant observation using qualitative methods, and analysis of questionnaire responses via quantitative methods.

Maxwell, Bashook and Sandlow (1986) combine the two methods in educational research. The differences between scientific and artistic (qualitative) research in education is discussed by Eisner (1981). He suggests that turning to qualitative research to satisfy the uneasiness caused by shortcomings in quantitative approaches will prove inadequate, as the issue is not the contrast between the two approaches, but rather the world in which the research takes place. 'With both we can achieve binocular vision. Looking through one eye never did provide much depth of vision' (Eisner 1981, p9).

4.4 RESEARCH METHODS IN INFORMATION SYSTEMS

There are two important considerations when embarking upon research in the information systems field. These are; first, the research addresses an area of importance to the industry, and secondly, that information gained from the research is able to be applied in practice within the industry. Research in a field such as information systems can be of great benefit to organisations, providing the subject of the research is of significance to the industry. Jarvenpaa, Dickson and DeSanctis (1985) believe that research designs are considered inappropriate when they do not address an important problem in the field; (possibly the word 'opportunity' should also be added here). Information systems is a very practical field and it is also

important that research is able to be applied into the 'real world'. Galliers and Land (1987) stress the need to apply the knowledge gained in IS research by suggesting this be a measure of the research's success.

Consistent technological change directly affects the information systems area, and new innovations are constantly emerging from the information systems industry. New products and techniques in the IS field are being developed based upon problems or opportunities faced by the application of technology into business situations. The changing character of technology and its influence on information within organisations over time has led the security function into a more sophisticated technical era. The integrity, availability, confidentiality and authenticity issues relating to information and information systems is a contemporary issue and research into this area necessitates the study of the planning and management processes within the organisation itself. Many factors influence the security of information and its related systems, hence it is necessary to examine the organisation in its immediate natural setting, rather than a simulated or laboratory situation.

The methods utilised in research within organisational settings has moved away from the more highly structured, quantitative traditional approaches to 'softer' more qualitative methods where more human and social factors can be considered. According to Bawden and Zuber-Skerritt (1991) this shift is part of a move from a product concentration to a process orientation, with the 'human factor' now assuming pre-eminence as a factor of production. Peile (1994) sees this as a focus on process rather than content. This trend has been seen in the emergence of qualitative research methods in the information systems area in the past decade in particular.

The notion that we, IS researchers, should be generating ideas, theories and hypotheses rather than simply testing them is offered by Fitzgerald, Hirschheim, Mumford and Wood-Harper (1985), and anything which restricts or constrains this process is inappropriate for the IS environment. Bakos and Treacy (1986) call for IT researchers to move beyond theoretical frameworks towards explanatory models of the underlying phenomena. Franz and Robey (1984) suggest that phenomenon should be studied in its context in the IS domain. This they call "idiographic"

research, which involves examination of a single event or entity, rather than seeking general laws, as characterised by research in the exact sciences. This view is also supported by Kaplan and Duchon (1987) who state that qualitative methods are characterised by the detailed observation of, and involvement of the researcher in, the natural setting in which the study occurs. In addition, they point out that such qualitative strategies emphasise an interpretive approach which uses the data gathered to not only pose, but also resolve research questions.

Galliers and Land (1987) believe that empirical research in the IS domain often leads to inconclusive or inapplicable results. They argue this stems from the need to apply values to variables, often leading to the exclusion of relevant factors difficult to value. In addition, they state the use of statistical tests implies a preciseness of measurement that is often not sustainable and could actually be misleading (Galliers and Land 1987, p900). Further, Lowe (1991) suggests the models of objective, academically detached, socially neutral inquiry are becoming increasingly inapplicable and that we need new ways of looking at the world, new ways of advancing knowledge and new ways of applying knowledge to complex problems. One of the main problems with the product-orientated traditional approaches is lack of adaptability to change, according to Bawden and Zuber-Skerritt (1991), and change is inevitable in complex and dynamic organisational situations.

Due to the social nature of systems and the complex and dynamic activities and issues associated with information systems within organisations, there is much support for the continued use of qualitative research approaches in this field. However, Galliers and Land (1988) warn that lack of thought often goes into the selection of an approach adopted by IS researchers, and emphasise the importance of choosing an appropriate methodology in a given situation. A researcher must choose the approach which best fits the problem under consideration and the circumstances of the researcher (Antill 1985).

Past research in IS has used qualitative approaches such as case study and action research extensively. The area of information systems is highly practical in nature, with a concentration on human-machine interaction. In their study of MIS research

strategies, Hamilton and Ives (1982) reported that two thirds of 532 published MIS research articles used qualitative rather than quantitative approaches. The typical focus of these articles was on a single variable, and case studies were the most commonly used method.

Galliers (1987) searched out methods used in IS planning and found the use of surveys, case studies and interviews was predominant. The analysis by Benbasat, Goldstein and Mead (1987) illustrates the expanding use of case studies and action research in IS research and clearly indicates a preference for interviews as the data collection method together with an exploration and explanation as the research thrust. Action research, in particular, produces findings that are pertinent and useful in information systems (Baskerville, 1998).

Keen (1984) also supports the use of qualitative approaches in IS research. He believes that IS researchers need not only a strong grounding in a reference discipline but also the ability to use descriptive, case-centred approaches to identify general trends and formulate these into recommendations and methodologies.

One of the most prominent qualitative methods used in social and human orientated research is action research, and the use of this method appears to have increased over the past decade in particular in the psychology, agriculture, education, nursing, management and information systems areas (see for example, Avison and Fitzgerald 1995; Avison and Wood-Harper 1990; Carr and Kemmiss 1986; Dick 1992 and 1993; Forbes, 1992; Galliers 1991; Harker 1991; McKernan 1991 and 1992; Perry and Zuber-Skerritt 1991; Wilson 1990; Woog and Turner, 1992).

Action research provides a people-orientated, scientific process for addressing real bottom-line issues, and has been used for over fifty years throughout the world in industry, government, education, community development and environmental monitoring and control (Passfield 1991).

The following sections discuss the case study and action research methods prior to presenting the overall design of this particular research.

4.4.1 Case Study

"A case study examines a phenomenon in its natural setting, employing multiple methods of data collection to gather information from one or more entities (people, groups, or organisations). The boundaries of the phenomenon are not clearly evident at the outset of the research and no experimental control or manipulation is used." (Benbasat, Goldstein and Mead 1987, p370). Eisenhardt's (1989, p534) definition is slightly different - ie, "the case study is a research strategy which focuses on understanding the dynamics present within single settings". In her view, case studies typically combine data collection methods such as archives, interviews, questionnaires and observations; and the evidence may be either quantitative or qualitative or both. Case studies can be used to solely provide description, or to test and generate theories. She states "when a pattern from one data source is corroborated by the evidence from another, the finding is stronger and better grounded" (Eisenhardt 1989, p541).

Case research is particularly appropriate in areas where research and theory are at their early stages, and situations where experiences of the actors are important and the context of the action is critical (Benbasat, Goldstein and Mead 1987). The key characteristics of case studies are illustrated in Table 4.1.

Benbasat, Golstein and Mead (1987) suggest the following questions be asked when deciding whether the case study approach is appropriate:

1. Can the phenomenon of interest be studied outside its natural setting?
2. Must the study focus on contemporary issues?
3. Is control or manipulation of subjects or events necessary?
4. Does the phenomenon of interest enjoy an established theoretical base?

The case study method has been used extensively in IS research in the past according to Hamilton and Ives (1982). Some widely publicised examples include studies by

Benbasat, Goldstein and Mead (1987), Bourgeois and Eisenhardt (1988), Dutton (1981), Franz and Robey (1984), Fulk and Dutton (1984), Gersick (1988), Harris and Sutton (1986), Hirschheim (1985), Ives and Olson (1981), Kaplan and Duchon (1987), Keen, Bronsema and Zuboff (1982), Markus (1981), Mintzberg and McHugh (1985), Pyburn (1983), and White (1984).

1. Phenomenon is examined in a natural setting
2. Data are collected by multiple means
3. One or few entities (person, group, or organisation) are examined
4. The complexity of the unit is studied intensively
5. Case studies are more suitable for the exploration, classification and hypothesis development stages of the knowledge building process; the investigator should have a receptive attitude towards exploration
6. No experimental controls or manipulation are involved
7. The investigator may not specify the set of independent and dependent variables in advance
8. The results derived depend heavily on the integrative powers of the investigator
9. Changes in site selection and data collection methods could take place as the investigator develops new hypotheses
10. Case research is useful in the study of 'why' and 'how' questions because these deal with operational links to be traced over time rather than with frequency or incidence
11. The focus is on contemporary events

Table 4.1: ***Key Characteristics of Case Studies***
Source: Benbasat, Goldstein and Mead 1987, p371

The case study approach is well-suited to IS research for the following reasons (Benbasat, Goldstein and Mead 1987):

- the information system can be researched in a natural setting, enabling the researcher to learn about state-of-the-art and generate theories from practice,
- allows researchers to answer how and why questions in order to understand the nature and complexity of processes taking place,

- an appropriate way to study an area where few previous studies have been carried out.

The case study method is also well suited for understanding the interactions between information technology related innovations and organisational contexts (Darke, Shanks and Broadbent 1998).

4.4.1.1 Strengths and Weaknesses of Case Studies

Case studies enable the researcher the capture reality in greater detail, according to Galliers (1991), together with the ability to analyse a greater number of variables than with more highly structured methods. Eisenhardt (1989) discusses the creative insight which can be gained from using case studies, emerging from an 'unfreezing' of thinking. She also believes that the emergent theory from case studies can be testable with measurable constructs, and that case studies often produce theory closely reflecting reality due to its concentration on evidence.

Because case studies study phenomena within their natural environment a much more comprehensive analysis of the total situation is possible, enabling the researcher to build theories following repeated observations of similar behaviour (Benbasat, Golstein and Mead 1987).

However, Eisenhardt (1989) warns that researchers commencing with preordained theoretical propositions may bias and limit the findings. Instead, she recommends that researchers identify a research problem and potentially important variables (having referenced the related literature), and avoid defining specific relationships between variables as much as possible. Eisenhardt also states that people are notoriously poor processors of information and there is a danger that researchers may reach premature and possibly false conclusions as a result of processing biases. She suggests the use of cross-case comparisons to identify similarities and differences plus patterns in sources of data.

Lee (1989) and Galliers (1991) see several problems with the use of the single case study in IS research, including the ability to replicate the study, and the ability to

extend the findings to other settings. Lee suggests that using additional case studies that test the theory in those other settings will allow the theory to be generalisable. This also applies to laboratory experiments, statistical experiments and natural experiments; ie. the same in IS research as in the natural sciences. Lee believes IS case studies are capable of achieving the same scientific objectives through different means.

The problem of generalisation is also addressed by Einsenhardt (1989) who suggests that selection of an appropriate population will control extraneous variation and help to define the limits for generalising the findings. Prior to offering generalised patterns across cases, Eisenhardt recommends the researcher become intimately familiar with each case as a separate entity. This enables the unique patterns of each case to emerge before generalisations are made.

Another problem with case study research is the excessive amounts of data collected, and researchers have no standard format for descriptive data gathered (Eisenhardt 1989). Galliers (1991) and Benbasat, Golstein and Mead (1987) highlight the problem of lack of control of variables, and the possible bias brought to the situation by the researcher or the researcher's interpretation of events and data. The use of triangulation of methods has been recommended to minimise this particular shortcoming.

4.4.2 Action Research

Action research can be defined as a paradigm, a methodology, a method or a tool, depending on the way it is applied within a given situation. At the highest level, Dick (1993) suggests action research is a research paradigm within which there are several recognised methodologies, and each methodology uses specific tools for information collection and interpretation. Figure 4.1 illustrates this concept.

For example, within the action research paradigm Dick cites a number of recognised methodologies, including Checkland's (1981) Soft Systems Methodology. The same

types of tools are generally used by more than one methodology and include interviewing, observations, content analysis, etc.

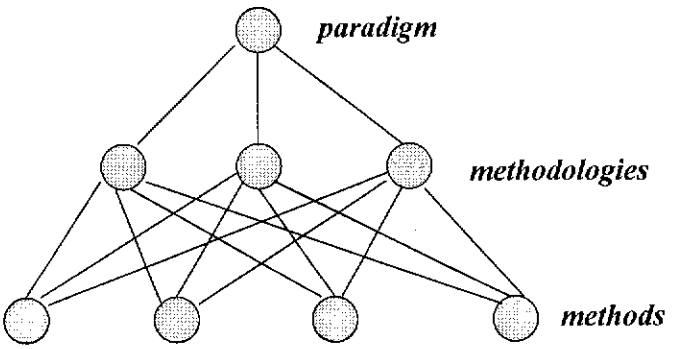

Figure 4.1: Paradigm, Methodologies and Methods (Dick, 1993, p11)

"Action Research simultaneously assists in practical problem-solving and expands scientific knowledge, as well as enhances the competencies of the respective actors, being performed collaboratively in an immediate situation using data feedback in a cyclical process aiming at an increased understanding of a given social situation, primarily applicable for the understanding of change processes in social systems and undertaken within a mutually acceptable ethical framework" (Hult and Lennung 1980, p247)

According to McKernan (1991, p43) action research is "systematic inquiry carried out by practitioners experiencing difficulties in order to understand, and/or solve, these problems so as to improve the quality of human action in social settings." The social setting is an important factor in action research, as different social settings could produce different results with the same stimuli (Baskerville and Wood-Harper 1998).

The perceived illusiveness of action research is illustrated by the following quote: "... pinning down just what action research *is*, is like nailing a jelly to a ceiling and when you're walking around with a hammer in your hand, everything looks like a nail" (Jones 1991, p96).

There are two slightly different opinions regarding the minimum set of activities comprising the action research approach. The first portrays three elements, planning, acting and reflecting, (Dick 1993). The second group suggests four elements, planning, acting, observing and reflecting (Carr and Kemmis 1986; Kemmis and McTaggart 1988; McKernan 1991). Other authors present action research in five stages (see Baskerville and Wood-Harper 1996). The essence of action research is not, however, in the number of activities, but its cyclical nature and feedback mechanism. Figures 4.2(a) and (b) illustrate the major stages of action research and its cyclical nature.

The act of critical reflection is an important aspect of the cyclical and spiral nature of action research. Kemmis and McTaggart (1988, p10) summarise the approach as follows:

"An action research group undertakes to collaboratively:

- develop a *plan* of critically informed action to improve what is already happening,
- *act* to implement the plan,
- *observe* the effects of the critically informed action in the context in which it occurs, and
- *reflect* on these effects as a basis for further planning, subsequent critically informed action and so on, through a succession of cycles."

As this quote suggests, the reflection or review process feeds data back to the planning stage of the next cycle. This feedback gives guidance for the next stage of the research, and the cyclic approach aids the uncertainty element of the research, where later cycles build on earlier ones. Swepson and Dick (1993, p7) suggest that each cycle develops greater precision about the research question, the methods and the conclusions.

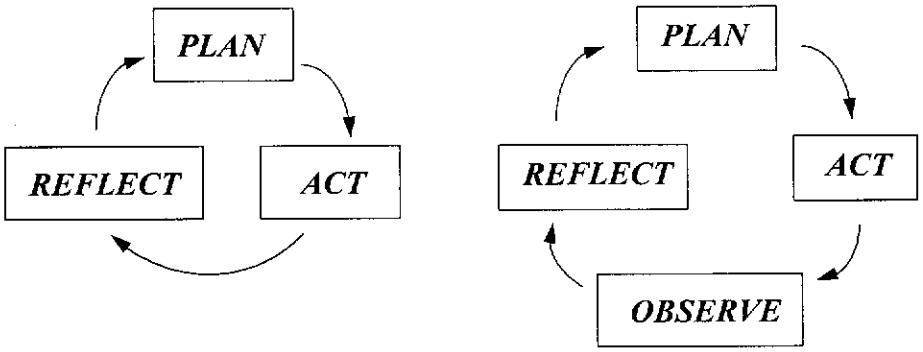

Figure 4.2: Action Research Steps

(a) three stage approach (b) four stage approach

The dual aims of *action* and *research* are highlighted by numerous authors (Dick 1993; Passfield 1991; Wilson 1990). In a bid to solve problems experienced in the 'real world', researchers plan, act and critically reflect on their actions in order to bring about change, and at the same time increase understanding and contribute to scientific knowledge. Wilson (1990) suggests action research simultaneously brings about change in the project situation (the action) while learning from the process of deriving the change (the research).

The linking of action and understanding is seen by Henry (1991) as a link between theory and practice. Taking action leads to a better understanding of the situation, and a better understanding leads to more prudent action. This suggests the research situation becomes clearer as continual feedback develops a fuller picture within the spiral. A spiral where each new turn builds upon the knowledge gained from the previous turn is referred to as the 'hermeneutic spiral' in the work of Gummesson (1991). The researcher has devised Figure 4.3 to illustrate the increasing knowledge gained via the spiral concept.

Hult and Lennung (1980) suggest the choice of techniques and methods should depend upon the nature of the problem, and any valid and reliable method for diagnosis, model-building, deduction, data collection, data analysis and evaluation may be used. The action research method has been used extensively in information

systems research and the Soft Systems Methodology (Checkland 1981; Checkland and Scholes 1990) frequently goes hand-in-hand with the use of the action research paradigm in IS settings.

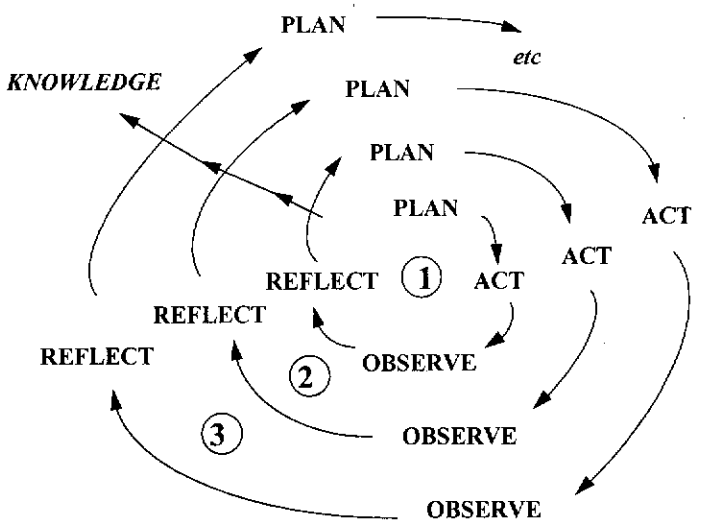

Figure 4.3: The Spiral Process of Action Research

The soft systems approach is based upon systems theory, and incorporates socio-technical aspects into the analysis of human activity systems. User participation and critical thinking are basic elements of this approach, and action research provides an ideal mode to achieve its goals.

Checkland (Checkland and Scholes 1990; Checkland 1991) recognises the lack of an intellectual framework defining the nature of research lessons within action research and its subsequent vulnerability to criticism by positivists. This appears to be due in part to the inability of action research to test hypotheses in the classical laboratory setting. "Action research requires involvement in a problem situation and a readiness to use *the experience itself* as a research object about which lessons can be learned by conscious reflection" (Checkland and Scholes 1990, p16).

In order to address this shortcoming, Checkland prescribes the following steps. First, the researcher selects a real-world situation with relevant research themes. Next it is necessary to negotiate the respective roles of the researcher and people in the

problem situation. The researcher must then declare the framework of ideas and the methodology in which they are embodied. As the research progresses, experience is accumulated in the unfolding situation to help bring about changes deemed improvements. This experience is accumulated, and upon completion of the task the researcher exits the situation and reviews the experience in order to extract the various kinds of lessons. This process is illustrated in Figure 4.4.

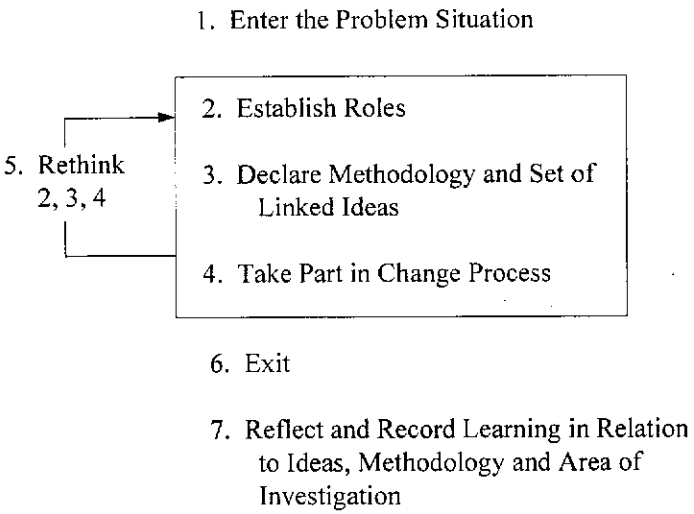

Figure 4.4: Action Research Process (source: Checkland, 1991)

The above framework should fulfil two purposes: first, to provide insights about the perceived problems leading to practical help in the situation; and secondly, that the experience gained in applying the framework will contribute to its gradual improvement (Checkland and Scholes 1990).

The people directly involved in the situation under study are stakeholders, and should be involved in the process of change regarding that situation. Argyris, Putnam and Smith (1985) believe one of the crucial elements of action research is a collaborative process between researcher and actors in the situation. Therefore, action learning is a partnership between the action researcher and the stakeholders, or actors, and each has a role to play. According to Hult and Lennung (1980), the action researcher contributes methods, a pre-understanding of the problem as well as intervention

skills. The client contributes his understanding of the specific situation and its idiosyncrasies. The researcher and participants are jointly responsible for the outcomes of the exercise, even though they play differing roles.

Drinan (1991) highlights the need to create an environment where all individuals involved become real participants in the process; being encouraged to confront issues, identifying questions that need to be asked, and contributing ideas in jointly searching for answers. Collaboration between the researcher and client staff members is essential if the researcher is to successfully utilise essential knowledge about the organisation held by those participants (Baskerville 1997a). Where change is a desired outcome Dick (1993) believes participation can generate greater commitment and action from those involved in the action research. This is because change is more easily achieved if people are committed.

Such collective action is supported by Passfield (1991) who reasons action research is a group activity. He states managers belonging to the focal group should be intimately involved in all stages of the research activity which is designed to improve their management practice and their situation. Kemmis and McTaggart (1988) suggest that participation also be widened from those most directly involved to as many people as possible affected by the practices concerned.

McKernan (1991) believes that action research is a challenging mode of inquiry, and as such, methodology is crucial to its development. He suggests the following framework of methods be considered as contributors to the methodology:

1. observational methods: eg rating scales, participant observation, checklists, photography, etc.
2. Survey/Self-Report Techniques: for example interviews, questionnaires, etc.
3. Narratives: analytic memos, diaries, field notes, case studies, anecdotal records, dialogue journals, etc.
4. Discourse Analysis: constraints analysis, episode analysis, dilemma analysis, document analysis, content analysis, etc.

5. Pedagogical Techniques: action inquiry seminars, brainstorming, role-playing, discussion, neutral chairperson, etc.
6. Critical-Evaluative Methods: triangulation, quadrangulation, lesson profiling, collegial review, discourse evaluation and others.

(McKernan 1991, pp 43,44)

4.4.2.1 Strengths and Weaknesses of Action Research

Action research gives permission to participants to question the perspectives, beliefs and values encountered in the activity, and that nothing within the agreed boundaries is sacred according to Drinan (1991). He reasons such an approach liberates the radical or serendipitous answer and encourages observation creating the truly new. The ability to create the truly new, in the researcher's view, will depend on the *willingness* of the participants to view the problem situation from different perspectives, putting aside assumptions and belief systems that have previously provided a basis for viewing the situation.

The understanding and learning processes within an action research situation should give the participants an enlarged kit of skills and competencies they may then adapt to new situations. This emphasises that people should be active participants in addressing their situations, rather than passive recipients of prescriptions and formulae (Drinan 1991). Perry and Zuber-Skerritt (1991) suggest action research is a highly effective process for developing the managerial competencies required by today's managers. Involvement in action research increases managers' understanding of their practice and their situation. The skills gained from the action research experience thus empowers participants to manage change in their ongoing situation.

If action research is to be credible *research*, it must be a rigorous intellectual process, and one of the most common criticisms of action research as an acceptable research methodology is its lack of apparent rigour (Dick 1992 and 1993; Jones 1991b). This criticism has been valid in many previous action research studies. Dick (1992) reports a further shortcoming of action research is its relative lack of economy in both conduct and reporting. In addition, "a common criticism of action research is its

lack of generalisability sometimes called external validity" (Dick 1993, p39). Galliers (1991) also highlights the difficulty in generalising given the problems of acquiring similar data from a statistically meaningful number of cases.

In Dick's view the generalisation problem can be described as a trade-off between local and global relevance (Dick 1993). By being responsive to the local situation, one may possibly sacrifice global relevance. Alternatively, you can pursue global relevance at all costs, even at the expense of denying opportunities for local change. He suggests that there is also a trade-off between universality of principles and universality of application. Where a finding is a universal or near-universal principle; it is hard to apply on its own, because it considers only a limited set of variables. On the other hand one needs to treat it flexibly when translating it into other settings.

Galliers (1991) also presents the possibility of different interpretations of events by individuals involved in the research, thus raising the question of possible bias. Ethics are a further important issue in Galliers' analysis of weaknesses of action research.

The rigour of conclusions reached using an action research approach can be assured by two activities in particular: the use of multiple sources of data or 'triangulation' (Dick 1992; Jick 1979; McKernan 1991; Swepson and Dick 1993); and by testing in later cycles tentative interpretations from earlier cycles (Dick 1992; Swepson and Dick 1993). Dick (1993, p12) believes that the spiral process which forms part of action research allows both responsiveness and rigour at the same time. The effectiveness of action research depends upon using brief and multiple cycles (and cycles within cycles). Previously Dick (1992) recommended at each cycle multiple sources of information be gathered using different methods, different informants, different researchers, or overlapping data from single informants. In addition, within each cycle he suggests attention be focussed on agreements and disagreements within the two or more data sets, and between cycles it is recommended that the researcher seeks out data which challenges or is at odds with previous interpretations. Each new cycle then begins by refining the questions and methodology in the light of the previous cycle.

One of the main advantages of action research is its responsiveness within the research situation. Qualitative methods generally are seen to lack repeatability, possibly due to the affect of the human element and the dynamic nature of the organisational situation. According to Dick (1993) replicability and responsiveness are hard to achieve at the same time because you trade off one for the other. Traditional research sacrifices responsiveness in the interests of achieving replicability, whereas action research desires responsiveness more than replicability, as it is directly linked with action within the research.

Action research is considered a method of change, and most appropriately applied where change is desired. The consequences of using action research can thus be dangerous, according to Drinan (1991, p93) who states "action research is potentially subversive in that it may lead to radical organisational and social change." It follows, then that the researcher must also be aware that he or she takes on the responsibility for change as well as for research (Dick 1993).

Action research is not an appropriate approach for all research situations. Conventional methods are more appropriate where responsiveness is not demanded in the research situation. Morgan and Smircich (1980) discuss the use of traditional and action approaches to research and offer the following example:

> "Participant observation in the hands of a positivist may be used to document the number and length of interactions within a setting, but in the hands of an action theorists the technique may be used to explore the realms of subjective meaning of those interactions."
>
> (Morgan and Smircich, 1980, p98)

Perry and Zuber-Skerritt (1991) believe positivist research methods are appropriate for clearly defined hard systems, while action research is appropriate for the soft systems of management practice. Dick (1993) suggests that it is more appropriate than mainstream research methods in situations requiring responsiveness, flexibility and action. Unlike traditional research, knowledge is acquired, tested and used

through direct involvement in organisational change and there is no delay between discovery of knowledge and its use in practice (Passfield 1991). The ideal domain for the application of action research as presented by Baskerville and Wood-Harper (1996) is characterised by:

- Active involvement of the researcher, with expected benefits for both the organisation and researcher,
- Immediate application of the knowledge gained, and
- A cyclical research process linking theory with practice.

Galliers (1991) presents a taxonomy of approaches for information systems research (see Figure 4.5) which distinguishes between scientific and interpretivist approaches. It gives guidance to researchers regarding the suitability of different approaches in the context of the particular topic under study. Galliers considers the focus of the research, (having an impact on society, an organisation or group, or an individual); whether the concentration is on technological or methodological factors; and the process of theory building, testing or extension.

	Modes for traditional empirical approaches (observations)					Modes for newer approaches (interpretations)				
OBJECT	Theorem Proof	Laboratory Experiment	Field Experiment	Case Study	Survey	Forecasting and Future Research	Simulation and Game / role Playing	Subjective / Argumentative	Descriptive / Interpretive (inc. Reviews)	Action Research
Society	No	No	Possibly	Possibly	Yes	Yes	Possibly	Yes	Yes	Possibly
Organisation/ Group	No	Possibly (small groups)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Individual	No	Yes	Yes	Possibly	Possibly	Possibly	Yes	Yes	Yes	Possibly
Technology	Yes	Yes	Yes	No	Possibly	Yes	Yes	Possibly	Possibly	No
Methodology	No	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
Theory Building	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Theory Testing	Yes	Yes	Yes	Possibly	Possibly	No	Possibly	No	Possibly	Possibly
Theory Extension	Possibly	Possibly	Possibly	Possibly	Possibly	No	No	No	Possibly	Possibly

Figure 4.5: IS Research Approaches: A Revised Taxonomy (source: Galliers 1991, p168)

Referencing this model, it can be seen that the case study method is appropriate for a project impacting an organisation, and also where the concentration is on the process (methodology) rather than the technology itself. Case studies are also suitable for theory building, but there are some reservations regarding its appropriateness for theory testing and extension. Action research is also appropriate for an organisational setting, concentrating on methodology rather than technology. Galliers also suggests that action research is suitable for theory building, and possibly also for theory testing and theory extension.

4.4.2.2 Action Research for Theses

Action research has adequate rigour and a long tradition according to Dick (1993) and is used frequently for masters and doctorate theses in a number of disciplines (see Dick 1993; Kemmis and McTaggart 1988; Perry and Zuber-Skerritt 1991). Action research used in Masters and Phd theses should consist of three integrated stages, the thesis research stage, the core action research project, and the thesis writing stage (Perry and Zuber-Skerritt 1991). Figure 4.6 illustrates this approach.

Whereas a Masters research project would possibly only require one cycle, according to Perry and Zuber-Skerritt (1991), the core of a doctorate action research project would need to progress through at least two or three cycles to uncover a distinct contribution to knowledge. They also suggest that although these cycles do not have to involve the same workgroup, it is important that the understanding gained in the reflection phase of the first spiral in the first workgroup be transferred to the planning phase of the first spiral in the next workgroup.

Perry and Zuber-Skerritt (1991) also present the view that doctorate research (in the discipline of management) should be emancipatory action research, rather than technical or practical action research. Emancipatory research has strategic action as its core, proceeding through the spiral of planning, acting, observing and reflecting, and involves participation and collaboration in all phases of the research.

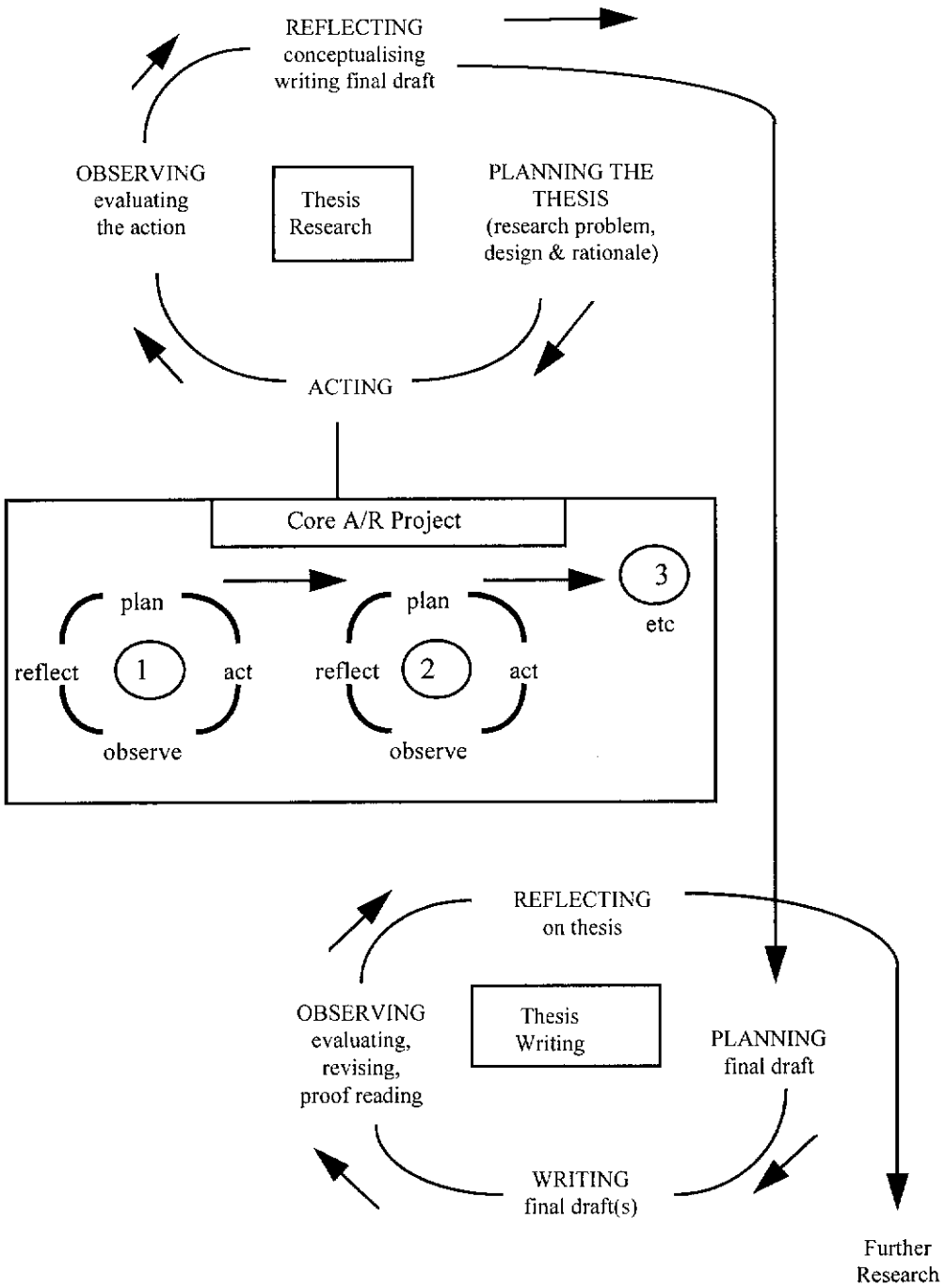

Figure 4.6: Action Research in Theses

(source: Perry and Zuber-Skerritt 1991, p76)

On the other hand, technical and practical action research has hard boundaries, with less collaboration and participation. The following table illustrates the three types of action research in an education environment:

Type of Action Research	Aims	Facilitator's Role	Relationship between Facilitator and Participants
1. Technical	- effectiveness / efficiency of educational practice - professional development	Outside 'expert'	Co-option (of practitioners who depend on facilitator)
2. Practical	- as (1) above - practitioner's understanding - transformation of their consciousness	Socratic role, encouraging participation and self-reflection	Co-operation (process-consultancy)
3. Emancipatory	- as (2) above - participant's emancipation from the dictates of tradition, self-deception, coercion - their critique of bureaucratic systemalisation - transformation of the organisation and of the educational system	process moderator (responsibility shared equally by participants)	Collaboration

Table 4.2 Types of Action Research and their Main Characteristics (source: Perry and Zuber-Skerrit, 1991: after Carr and Kemmis 1986)

Based upon the preceding discussion, the elements which set action research apart for doctorate level projects from other research using action research are:

- Use of a core action research project within the thesis planning and development cycle,
- Progression through two or three cycles of the action research spiral, and
- Emancipatory action research, involving a high level of collaboration and participation.

4.5 OVERALL RESEARCH DESIGN

The progression of research steps chosen for this particular research is similar to the approach illustrated in Figure 4.7 below. Galliers (1991) suggests that the IS researcher commences with a research question which may then be followed by survey research. This stage leads to theory building, then case studies or action research to assist in the testing of these theories in a field environment. The findings then lead to theory extension, and the research may then cycle back to further case study or action research to test the extended theories in action.

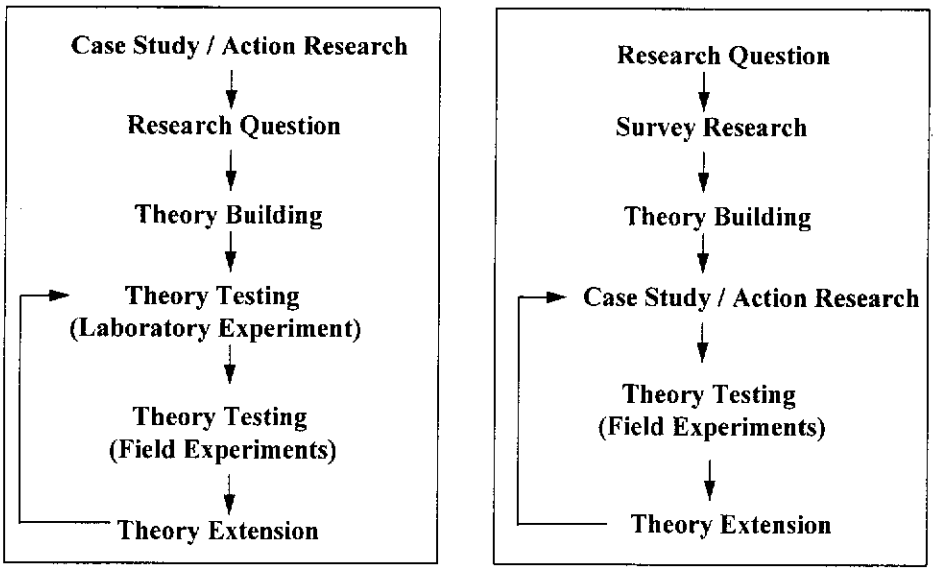

Figure 4.7: Use of Alternative IS Research Approaches in the Process of Theory Building (source: Galliers 1991, p170)

Howard (1988) suggests that research in IS should begin with exploratory studies and end with cross-validation of the new theory in a real life situation, proceeding in two phases: empirical and theoretical. The empirical or theory building stage involves identification of variables and development of concepts, propositions and models relevant to the problem. This stage attempts to focus the problem without offering a solution and contributes to the formation of untested theoretical propositions. The

theoretical stage is a stage of detailed theory building and testing in practice resulting in either rejection or validation of the theoretical propositions.

A similar approach has been used in this research project, the application of which fell into four main phases:

- Identification and analysis of, the current situation regarding the management of information systems security within business organisations
- Study of current models recommended in the field of IS security management
- Development of an alternative management approach to information systems security, and
- Learning from the practical application of the model in an organisational situation.

Wood (1995) explains the design of her doctoral thesis, consisting of both qualitative and quantitative research methods. It consists of three components, the first is a multidimensional Likert-scale instrument, the second a survey eliciting both qualitative and quantitative data, and finally a field research component.

Utilising Howard's (1988) framework as a reference point, the empirical stage of the current research involved the first two phases listed above. The first phase involved an in-depth study of sixty business organisations within Australia to identify how information systems security is currently managed. Security and IS audit literature was searched to obtain a comprehensive list of factors to be studied and evaluated, including recommended security management measures, plus problem areas within the information security arena. Each organisation was studied in detail and information gathered on the current methods employed. The effectiveness of security measures implemented were evaluated and rated on a Likert scale to enable some statistical analysis to be carried out. The findings from the statistical data together with qualitative data gathered via interviews and observations during this first phase were used in the formation of the new model.

Phase two commenced with a study of security management models recommended from the literature. The models identified were analysed for content, process and application. The *content* features of these models studied included the level of

management application, the extent of security coverage and the amount of detail given in the material. The consideration of *process* included analysis of the method or approach recommended for transforming the content into practice and the comprehensiveness of the transformation actions involved. This stage also included study of the integration of the content and process. Details of the application of each model were then studied to ascertain the extent of testing of the models into a live and practical environment.

The theoretical stage embraced the final two phases, in an effort to build and apply a new model. Phase three involved the development of a new approach to the management of information security. This new model incorporated the findings from phase one together with the conclusions from the model analyses in phase two. The final phase involved the application of the new model into a live organisational situation.

4.6 RESEARCH THEME

Checkland (1991) advises that in action research the researcher is not dealing in hypotheses, but in research themes within which lessons can be sought. Swepson and Dick (1993) suggest that at the start of a study it is difficult to know precisely what research question to pursue. In fact, using action research the initial research question is likely to be fuzzy (Dick 1993), and this is due to the nature of social systems. Dick goes on to suggest that when a fuzzy question is addressed with a fuzzy methodology, such as action research, then the best answer one can initially find must also be fuzzy. However, provided that the fuzzy answer enables the researcher to refine both the question and method (via a spiral process), then eventually precision can be found. "You don't need a research question or hypothesis at the start of a study beyond a wish to know how to improve the situation" (Dick 1992, p434).

This infers that a detailed set of hypotheses at the commencement of the research is not appropriate if action research is used, as this may influence the researcher's analysis and conclusions drawn. A preformed hypothesis may also reduce the

researcher's responsiveness to the research situation and restrict the breadth of possible questions and solutions. Dick states "if you are adequately responsive to the situation, you can't begin the exercise with a precise question. The question arises from the study." (Dick 1993, p13)

At the beginning of this research project, the research question was quite indistinct, except for the recognition of a need to improve the management of information systems security within business organisations. As discussed in Chapter 2, the literature suggests this need is real, evidenced by the rise in rates of computer abuse, the reported absence of security measures within organisations, and a lack of security awareness.

The first research theme became clearer as the study progressed – to determine if the lack of information security management is a real issue in Australian organisations. Following the study of numerous organisations to see how security was actually managed in practice, it was found that security is generally poorly planned and managed. The lack of user involvement at all levels of the organisation appeared to be a major contributing factor. In addition, a general lack of awareness regarding security matters (possibly due to a lack of involvement) was also found, thus supporting the findings from the literature.

The need for an adequate method of planning and managing information security was apparent. In this context 'adequate' means a more socio-technical approach which incorporates higher user involvement. The search for possible information security management approaches found the majority of models were technical in focus with only a few truly socio-technical models. Unfortunately, the literature shows little evidence of successful practical application of these models. It is difficult to determine whether these models could, in fact, improve the management of information security.

Using Checkland's (1981) Soft Systems Methodology, a socio-technical model, the Orion Strategy was devised. In order to incorporate more social and human aspects into security management and learn from this experience, action research was used to

build and apply the Orion Strategy to an organisation in the health care industry. The health care industry was one of the poorest performing industries in the study of current information security management (see Chapter 5).

Thesis Chapter	Stage in Galliers (1991)	Stages in this Research
2	Research Question	Is the lack of information security management a problem? Results of the literature search say "yes".
4	Survey Research	Is the lack of information security management a real issue in Australian organisations? Results of the survey say "yes". There is lack of user involvement in, and lack of ownership of information security.
3 6	Theory Building	Search to find an adequate socio-technical model was unsuccessful. Majority of approaches are technical. Build the shell of a new socio-technical approach, the Orion Strategy.
7	Action Research	Learn from the application of the Orion Strategy in a live, organisational setting. Modify and enhance the model during its application.
8	Theory Testing	Has the Orion Strategy resulted in an improvement in information security management? Indicators from the organisational setting under study say "yes".
9	Theory Extension	Identify emerging themes. Clarify the need to apply the Orion Strategy in other organisations and other industries to learn further from its application.

Figure 4.8: Development of the Research Themes

The problem situation recognised as a point of commencement was the poor management of information security. The aim of the research was to improve the problem situation, i.e. improve the management of information security. The application of the Orion Model was to learn from, and aid this improvement process.

The evolution of the research theme, using the Theory Building process illustrated in Figure 4.7 is illustrated in Figure 4.8. The Orion Strategy, incorporating high levels of user involvement, was used as the tool to learn about improving the management of information security.

4.7 CHAPTER CONCLUSION

Due to the socio-technical nature of the research at hand, both qualitative and quantitative research methods have been applied in this research. The case study method has been chosen for the gathering of information on the current state of information security management in organisations. Action research was chosen as the most appropriate tool for building and applying a new information security model.

5. INFORMATION SECURITY IN AUSTRALIAN ORGANISATIONS

5.1 CHAPTER INTRODUCTION

Previous discussion highlights the lack of information security management as reported by earlier studies, as well as the increasing problem of abuse via computer systems. As can be seen, these studies apply to business organisations in many areas of the world, each presenting similar findings. Studies carried out on Australian organisations have been spasmodic, with concentration on computer abuse (Benbow Masters and Cooper 1986; Kamay and Adams 1990, 1992; KPMG 1993, 1999a). A more comprehensive picture of the current status of information security management in Australian organisations was sought in an effort to determine practices which may ensure a more efficient and effective availability, integrity and confidentiality of corporate information.

5.2 RESEARCH AIMS AND APPROACH

The study described in this chapter was carried out within sixty Australian business organisations to ascertain the security measures currently implemented and any security problems these organisations have faced. It was anticipated that the information gathered would give a snapshot of the current state of security procedures and controls within each organisation participating in the study. In addition, the data collected on security problems would provide an indication of the extent of violations actually occurring, in spite of the controls already in place. Hence the results of this study will provide a picture of information security management currently in practice. It may then be possible to devise a means of improving security management and raising security awareness, if these were seen to be required.

5.2.1 Research Theme

The research undertaken at this stage of the thesis was one of investigation to ascertain the current state of information security management in practice within

business organisations. It was decided, therefore, that a research 'theme' would be more appropriate than a research 'hypothesis', as the derivation of a specific hypothesis that could be proven true or false would be difficult. In order to get a bigger picture of the present situation, the following general theme was posed, and data collected to shed some light on this particular area.

Research Theme *What is the level of action by management and user staff to ensure the integrity, availability and confidentiality of information?*

For such action to be taken, it is assumed that some awareness regarding security vulnerability or the need to assure integrity, confidentiality and availability has been recognised. As discussed in Chapter 2, past research has reported that levels of awareness regarding security vulnerability was low.

Conscious action, involving the planning, design and implementation of recommended security measures implies that managers and users are not only aware, but also have a commitment to security and an acceptance of responsibility for upholding the aims of data integrity, confidentiality and availability. In effect, to take action necessitates an awareness of vulnerabilities and threats and a commitment to reduce the associated risks. This concept is illustrated in Figure 5.1. The act of feedback stems from reviews of vulnerabilities, threats and risks and provides information increasing awareness.

Fowler (1996:157) suggests that a security culture must entail awareness, acceptance and action. The research theme indirectly embraces all these steps, as action cannot be taken until the earlier steps are undertaken. This study reviews the extent to which recommended security measures have been actioned within business organisations.

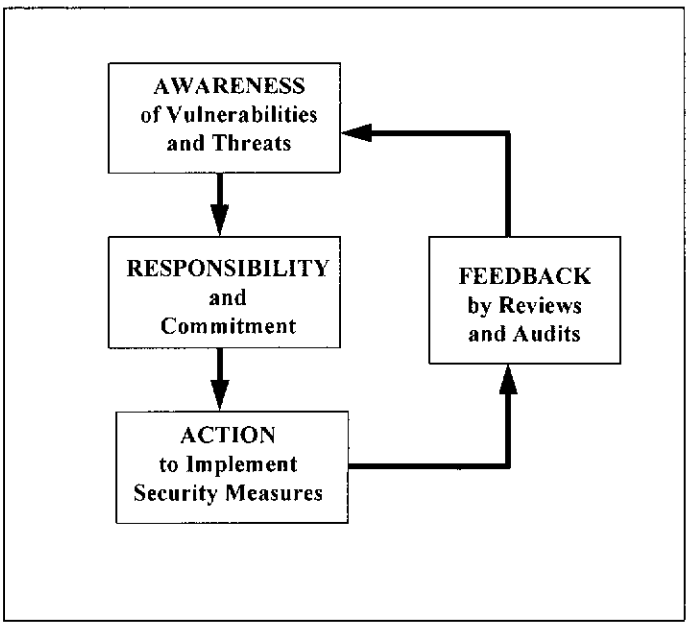

Figure 5.1: The Security Management Action Cycle

5.2.2 Research Design

Organisations to be studied were predominantly those who had participated in previous activities related to information systems. For example, study sites included organisations who had sent representatives to presentations or professional development courses conducted by the Australian Computer Society, or who had provided information systems planning and development project sites for undergraduate and post-graduate students of the university.

To be eligible for consideration, each organisation had to meet the following criteria:

- Management was willing to discuss information security matters freely with the researcher (within the agreement of confidentiality provided);
- Management was agreeable for IS and user staff to be interviewed;
- Management was agreeable to a security review of the organisation's current practices and procedures, and observation of day-to-day operations could be freely carried out by the researcher;

- Management provided all written documentation requested by the researcher, including policies, procedures, job descriptions, minutes of meetings, and the like;
- The organisation was using a multi-user, multi-tasking computerised information systems with a minimum of ten users;
- The organisation had the capacity and expertise to develop information systems in-house, using either their own staff or contractors;
- IS Development projects were organisational goal focussed and involved three or more analyst/programmers.

Information was collected via interviews with management, auditors, IS and user staff; review of written documentation, observations and site visits. This information was collated into predefined formats and rated according to a given scale (see Data section to follow). Statistical analysis was then carried out to determine significant factors and relationships.

5.3 DATA INCLUDED AND INFORMATION COLLECTED

Security measures reviewed in each organisation covered a range of management levels, from the corporate-wide down to the operational level within systems development and production environments. Also studied was the occurrence of security related problems along similar lines to previously reported studies. The data collection summary sheet which show both security measures studied and security problems experienced can be seen in Appendix C.1.

5.3.1 Variables Used in the Study

In line with the recommendations from the literature discussed in Chapter 2, data at a corporate level was collected on security policies, security planning activities, risk analysis and contingency planning, allocation of responsibility for security and its active supervision, security education, and quality assurance methods. These security measures implemented at the corporate level indicate executive management awareness of information as a corporate asset, and the importance of using security measures to assist in fulfilling the organisation's goals or mission. Corporate

security measures also suggest the commitment of management to security and the high level action they are willing to take.

Security measures implemented at an operational level reveal the action taken to ensure integrity, confidentiality and availability of information in the organisation by the implementation of procedures to support corporate security measures. The extent of implementation of operational security measures also indicate the associated awareness of security issues and commitment by managers and user staff. These measures indicate the importance of information in day-to-day procedures of the organisation and also illustrate the distribution of responsibility for its safekeeping and integrity. Operational security was studied by reviewing security responsibility assignment, backup procedures, logical access controls, physical access controls, log and error management, network and communications controls, change control and independent audits.

Security measures within the area of systems development and systems re-engineering (including business processing redesign) are extensions of corporate and operational security measures. Actions to implement these security measures reflect a desire for quality systems with continued integrity, availability and confidentiality of information. Controls at the systems development level include project management methods; development team composition; use of a development methodology; procedures for requirements specification, documentation and testing; design controls; walkthroughs; separated logical development, testing and production areas, and procedures for the transfer of new software systems to operational environments.

The effectiveness of each control studied was rated between one and five (in Likert style), according to how extensively the measure was implemented and actively monitored. A rating of one indicated the control was absent or not used, and a rating of five denoted the control was implemented effectively and consistently monitored (see Appendix C.2 for rating descriptions for each variable considered). Table 5.1 illustrates the security measures used in the study.

Corporate Security Measures	Description
Security Policy	Written, corporate-wide information security policy
Security Planning	Planning for information security at a high level
Risk Analysis	Analysis of risk for information assets
Contingency Planning	Disaster recovery planning for information assets and functions
Security Manager	Assigning responsibility for security to a senior staff member
Supervision of Security	Monitoring and active supervision of information security
Security Education	Security education and training programs
Quality Assurance	Methods and procedures to ensure quality assurance

Operational Security Measures	Description
Responsibility for Security	Distribution of responsibility for information security
Physical Access Controls	Security measures to limit access to physical assets
Logical Access Controls	Security measures to limit access to data and software
Systems Logs and Error Handling	System records of activities and error occurrences
Change Control	Controls to manage access and modification of software
Communications Controls	Protective measures to secure networked environments and electronic communications
Independent Audits	Audits of IS functions by independent personnel
Backups	Controls to ensure secure, on-site and off-site backups

Systems Development Controls	Description
Project Management	Project management of IS developments (and outsourcing)
Development Team Composition	Members of development teams, including users
Development Methodology	Methodology for the development process
Requirements Specification	Procedures for written definition of requirements
Systems Documentation	Standards for online and hardcopy documentation
Design Controls	Procedures and standards for designs, including controls
Walkthroughs	Regular reviews with stakeholders and peers
Testing	Procedures and standards for testing prior to implementation
Separate Environments	Distinct environments for development and operations

Table 5.1: Security Measure Variables Included in the Study

Security or management control problems relating to violation of data integrity, data privacy and continued systems availability were also collated for each of the organisations studied. Indicators of problems included the occurrence of data errors, data corruption, data loss, high systems maintenance and denial of use, unauthorised logical and physical access, fraud, sabotage, theft of computer and information assets and rogue code. The frequency of occurrence and impact of these problems was also rated on a five point Likert scale (see Appendix C.3). A rating of one indicated that the occurrence was frequent and the impact on the organisation severe. A rating of five, on the other hand, denotes there are no known occurrences of this problem with a corresponding lack of impact. Table 5.2 summarises the security problem variables used in this study.

Security Problems	**Description**
Data Error	Data errors caused by human or system problems
Data Corruption	Data corruption caused by humans (not sabotage) or system problems
Loss of Data	Loss of data
Denial of Use	System downtime, extent of maintenance
Lack of Documentation	Lack of system documentation, help facilities
Fraud	Fraud, embezzlement
Logical Access Violation	Unauthorised access to software and data, either internal or external
Physical Access Violation	Unauthorised access to physical assets, either internal or external
Software, Data Theft	Theft of Software and/or Data
Hardware Theft	Theft of computer equipment, facilities
Unlicensed Software	Illegal copies of software
Sabotage	Sabotage of hardware, software and/or data
Rogue Code	Virus, worms, etc, attacks causing damage to hardware, software

Table 5.2: Security Problem Variables Used in the Study

In all but a few organisations the ratings for security measures implemented and security problems reported were discussed and agreed upon with the managers and users interviewed. In a small number of cases the managers interviewed were only recently employed and did not have all the information required. In those cases the

ratings were discussed with IS auditors, and a rating was assigned on the basis of audit records and other appropriate documentation.

Several additional variables were deemed to be appropriate to be included in the study, in order to give a richer picture of the organisational situation and the information systems setting. These variables include the type of industry in which the organisation operates, the type of software platform used, how centralised were the systems, the impact of the system across the organisation, the sensitivity of the information handled, the organisation's experience with computerised systems, and the size of the system by number of users. Appendix C.4 summarises these variables. The additional variables are described below:

Type of Industry: The industry within which each organisation operates is a common factor to be included in studies of business enterprises. This factor may indicate trends or significant relationships for organisations in the same or related industries. The categorisation of industry types was taken from the previous study on security management by Benbow, Masters and Cooper (1986), encompassing agriculture, automobile, Australian government, banking and finance, conglomerates, education, food and beverage, general manufacturing, insurance, mining and metals, petroleum and chemicals, publishing and communications, retail and wholesale, state government, statutory authorities, textiles and footwear, transport and others. A number of additional industry groups were required to fully represent the sample used in the present research. These included building and construction, computing and technology, health and medical, and real estate. With this study limited to a sample of sixty organisations it is not possible to examine security measures and problems in each industry group. This measure does, however, show the representativeness of the sample.

Type of Software Platforms and Development: Organisational policies regarding the development of software, or purchase of pre-developed software modules was considered to be a factor that could have an effect on systems development controls. A security environment where all software is developed in-house using 3GL's (such as COBOL) will differ from one where 4GL's and more automated software

development tools are used. Similarly, a situation where software packages are modified to suit the organisation's requirements will require a different approach to the control of systems development.

Three categories are considered in this study, a 3GL development environment, a 4GL development environment, and a pre-developed package situation, regardless of modifications.

Span of Impact: The impact of non-availability of the computer systems was considered in the Benbow study of security in Australian organisations under three categories: minimal effect on company operations, inconvenience effect on company operations, and major effect on company operations (Benbow Masters and Cooper 1986). The importance of recognising the impact of non-availability and of errors due to the density of stored information is also suggested (by DOCIT 1988). Three levels of the span of impact are considered in this research, the first affects only the department within which the system resides, the second affects numerous departments, and the final level affects the whole organisation.

Sensitivity of Information Held: The sensitivity of the data held will depend upon the type of industry, the system itself and its major functions. The data stored on systems encompassing financial accounting or research and development information will commonly be more sensitive in nature than general information systems available to the public such as details of goods for sale and price lists. As previously discussed in the section on classification of information, it is important to recognise the sensitivity of the particular information held, or the parts of the systems that hold the most sensitive or valuable data.

A five level categorisation of information sensitivity was used in this study. The first level is restriction to only a selected number of individuals; the second, restricted to a named department or section; the third, restricted to a number of departments or sections; the fourth, restricted to use within the organisation; and finally, no restrictions as the information is for public access.

Maturity of Users: The maturity of users as measured by experience with computing systems has been a factor discussed by numerous authors. Allen (1995) suggests a six- staged model of IT maturity within organisations that ranged from the novice through to organisations where IT is considered a mechanism for improvement which is part of the organisation's mission and vision. A three staged categorisation of user maturity can be found in the work of Benbow, Masters and Cooper (1986, p6) - less than three years' experience, between three and eight years' experience, and more than eight years' experience. Unfortunately, the report does not explain why the authors considered the three and eight year limits significant for maturity considerations.

Orlandi (1986) uses the Gibson and Nolan (1974) model of electronic data processing growth to define the specific aims of information system security. He allocates the growth model to the dominant security aims or attributes i.e. reliability, integrity, vulnerability, confidentiality, privacy and security engineering. As Orlandi's theoretical model does not appear to have been applied and tested, it is not known whether information security is significantly related, in practice, to the stages of maturity. However, it is possible that the level of user maturity and experience in information systems could affect an organisation's awareness of security concerns and the implementation of protective measures.

Mahmood and Becker (1985) also used the Gibson and Nolan maturity model in relation to user satisfaction, and reported a significant relationship between the user satisfaction variables and the Gibson and Nolan growth variables. This research suggests that organisational factors should not be ignored in systems development, and that the maturity of the user with regard to computers should be taken into account.

As the Gibson and Nolan model of maturity is a well utilised tool in IS research, it was decided to use this model for this study. The original four-phased model was used, namely; initiation, contagion, control and maturity (Gibson & Nolan, 1974). During the initiation stage, the organisation determines those functions most fitting to be automated. The contagion stage is the expansion of computing into other

application areas. In the control phase, management implements controls around IT development, operations and management in a bid to monitor and control the application of technology within the business. The final stage, maturity, is characterised by a balance of short-term delivery with the recognition of investment for the future.

Number of Users: Few, if any, previous studies have included consideration of the number of users accessing the computer systems. In light of the recent explosion in networks and global communications, it was considered pertinent in this research to study any influence on security which may emanate from the size of the user population. At the time of data collection, the actual number of users was recorded, however, these figures were too disparate to perform meaningful statistical analysis. A minimum of ten users was required for inclusion in the sample. Three groups were formed; between 10 and 20 users, between 21 and 80 users, and more than 80 users.

Centralisation: To be most effective, information security needs to be tailored to the organisation's requirements, and this is particularly pertinent when considering highly centralised or decentralised computing environments. As discussed in the previous chapter, the use of networked and distributed computing environments makes it increasingly difficult for organisations to ensure the integrity, confidentiality and continued availability of information. The risk of errors, abuse, misuse and need for increased maintenance increases as access to data, software and computer power is distributed. The sophistication and technical complexity of networked systems is a contributing factor. Centralised storage of data and software has always been more easily controlled due to its concentration within a single physical and/or logical environment. Distributed or decentralised systems are more difficult to secure because of the numerous locations, often with differing physical and logical installations.

It was considered necessary, therefore, to look at an indicator of the extent of centralisation (or decentralisation) for the organisation's information system. A five level, sliding category was used, where level of one indicated total centralisation and level five indicated total decentralisation of hardware, software and data facilities.

5.3.2 Collection of Data

A number of interviews with managers, auditors, IS and general staff were carried out to gather the required information. Written material was consulted, including documents, policies and reports. Observation of practices was performed on site for each organisation studied. In the majority of cases the collection of data involved numerous visits to the site and observation of activities on several occasions. Triangulation (the use of multiple methods) was a feature of the data collection, with information being generally confirmed by more than one source, namely other parties, written documentation or through observation.

The ratings assigned for the implementation of security measures and the occurrence of security problems were jointly decided by the researcher and the managers and/or auditors at each site. This necessitated discussion and agreement upon appropriate ratings based upon the information gathered. Consistency across cases was also considered by the researcher in the final assignment of ratings.

5.4 DATA ANALYSIS AND FINDINGS

The research theme encourages both qualitative and quantitative analysis of security measures and the assignment of responsibility currently in place in participating organisations. Statistical analysis designed to illustrate significant relationships in the data included frequency distributions, parametric and non-parametric correlation coefficients (2-tailed), one-way ANOVA and crosstabulations. Factor analysis was also used as a means of summarising the security measures and problems experienced in the participating organisations. All analyses were accomplished using SPSS software. Qualitative analysis was also carried out from interview and observation notes. Appendix D summarises the interrelationships between the various measures of information security and problems.

5.4.1 Corporate Security Measures in Practice

Table 5.3 summarises the frequencies of ratings for corporate security measures. The existence of efficient and effective corporate security measures is low, with only 10% or less of organisations indicating the top rating for the security measures. Security policies were not common with the majority of organisations having little or no policies regarding security of information. Planning rarely appeared with the significant majority having little or no security planning. Risk analysis and contingency planning were generally addressed in a superficial manner with the original work in these areas not being updated or tested in the majority of cases.

The responsibility for security had in most cases been assigned to an individual. However, only a small proportion had given this responsibility to a senior staff member with the authority, expertise and financial resources to carry out the job effectively. Survey responses for supervision of security should reflect the figures of "security manager" however, very few organisations were actively monitoring security functions.

Corporate Security Measures	1 Does not Exist	2 Poor	3 Part Only	4 Good	5 Fully Active	Row Total %
Security Policy	46.7	16.7	15.0	13.3	8.3	100
Security Planning	78.3	11.7	3.3	5.0	1.7	100
Risk Analysis	26.7	23.3	38.3	6.7	5.0	100
Contingency Planning	26.7	28.3	36.7	3.3	5.0	100
Security Manager	10.0	23.3	28.3	28.3	10.0	100
Supervision of Security	30.0	21.7	20.0	26.7	1.7	100
Security Education	61.7	20.0	11.7	5.0	1.7	100
Quality Assurance	75.0	8.3	8.3	3.3	5.0	100

Table 5.3: Frequencies of Corporate Security Measures (% of organisations surveyed)

Security education was not a common corporate activity with few organisations running effective security education or training programs for their employees. The majority of participants had no education or training. Quality assurance programs were not recognised as important in a large proportion of organisations. No quality assurance program whatsoever was found in a large majority of organisations, and only a very small number of participants indicated a satisfactory level of quality assurance procedures.

Bivariate correlations on corporate security measures generally demonstrated significant relationships between corporate measures and security measures in all three groups - corporate, operational and systems development. An absence of a corporate security policy is significantly associated with a lack of most operational security measures and systems development controls. The prominent pattern evident is that organisations with poor corporate security measures also showed poor operational and systems development controls. The data therefore reflects the tendency for organisations to either implement most corporate security measures or none at all. See Appendix D for a summary of significantly related variables, and Appendix D.1 specifically for information regarding corporate security measures.

With the exception of security supervision and quality assurance, there was not a strong association between corporate security measures and the existence of security problems. Crosstabulations of security supervision and significant security problem variables generally suggested the occurrence of security problems where organisations have little or no security supervision in place.

With regard to the relationship between quality assurance and security problems there does not appear to be any emerging patterns from this analysis. The high number of organisations without any form of quality assurance program (75%) results in an uneven distribution of cell occurrences within related crosstabulations, and any interpretation must thus be made with care.

5.4.2 Operational Security Measures in Practice

Table 5.4 summarises the frequencies of operational security measures implemented by organisations. A rating of 4 or 5 for user responsibility for security occurred in a small number of organisations studied, whilst nearly one-quarter were rated at only 1. The majority of organisations had partially assigned responsibility to given users of the information or systems, however, security was predominantly regarded as an IS Department responsibility. Regarding physical security measures, more than half had little or no controls in place and less than one-quarter of participants were found to have good physical controls.

The majority of organisations had some form of logical controls in place, however, many of these were limited to only usernames and basic password. Just under half the organisations had reasonable levels of logical security measures implemented and effectively operational, i.e. ratings 4 and 5. Little or no controls in systems logs and error handling (ratings 1 and 2) was evident in nearly half the organisations studied. Change control was implemented and active in only a small number of organisations with many having little or no change control of software.

Operational Security Measures	**1** Does not exist	**2** Poor	**3** Part Only	**4** Good	**5** Active	**Row Total %**
User Responsibility for Security	23.3	36.7	28.3	8.3	3.3	100
Physical Access Controls	13.3	40.0	25.0	13.3	8.3	100
Logical Access Controls	5.0	31.7	16.7	36.7	10.0	100
System Logs and Error Handling	18.3	28.3	23.3	28.3	1.7	100
Change Control	20.0	16.7	26.7	30.0	6.7	100
Communications Controls	70.0	13.3	11.7	5.0	0.0	100
Independent Audits	43.3	11.7	5.0	25.0	15.0	100
Backups	0.0	23.3	20.0	35.0	21.7	100

Table 5.4: Frequencies of Operational Security Measures (% of organisations surveyed)

Network and communications controls were particularly poorly implemented in the majority of organisations studied, with only a few having effective measures in place. No network and communications measures were found in 70% of participant's systems, although this could be explained by the proportion of organisations with a tendency to centralise their software and data.

Organisations tended to either actively support independent audits or not carry them out at all. Backups were effectively carried out in just over half of the organisations studied. All organisations carried out some form of backup, however, many had very poor backup procedures.

Bivariate correlations demonstrated that operational security measures, with the exception of independent audits, showed significant relationships with the majority of corporate security measures and systems development control variables (see Appendix D.2). As expected, there was also a significant association between variables within the operational security group itself - where the absence of one operational security measures commonly occurred in the absence of other measures. It was further noted that a lack of operational security measures was frequently associated with a lack of corporate security measures and systems development controls. In addition, implemented and active operational security measures commonly occurred together with implemented and active security measures.

Independent audits were found to have limited association with other security measures, possibly because just under half the organisations studied did not undertake such audits. The conduct of independent IS audits did result in a significant association with security manager, and security supervision, possibly indicating that the appointment of a security manager and active supervision of the security function recognises the importance of performing IS audits.

Operational security measures relating to access to software and data in particular (namely logical access controls, system logs, change control and communications controls) were significantly correlated with security problems associated with the

integrity and availability of data, i.e. data corruption, data error, and loss of data (see far right hand column of Appendix D.2). The same security measures also indicated a significant association with logical violations to information systems. Other operational security measures (user responsibility, physical access controls, backups and independent audits) showed no discernible patterns of association with security problem occurrence.

5.4.3 Systems Development Controls in Practice

The frequencies of systems development controls are summarised in Table 5.5. It would appear that organisations were not consistent in the application of development controls with a minority of participating organisations achieving a rating of 4 or 5 for most measures. Project management was undertaken in some form in the majority of cases, however, many indicated a low level of project management activities. The involvement of users on the development team appeared to be either supported or rejected by participants, with a small proportion reported for the middle rating.

The majority of organisations reported using a recognised development methodology. On the other hand nearly one-third of organisations did not use a methodology regularly if at all. Effective procedures to ensure written requirements specifications for system developments were found in less than one-quarter of cases, with the majority showing poor or non-existent requirements specifications. The frequency of systems documentation relating to new systems was similar to requirements specifications.

Design controls were implemented effectively in less than one-quarter of organisations, whereas nearly three-quarters had little or no controls to ensure systems design was correct or appropriate. Walkthroughs were carried out effectively in nearly half of cases with just less than half undertaking few or none. Testing was effective and appropriate in only a small number of organisations, with more than half having little or no testing procedures and controls in place. Nearly half of the organisations had separate development and operational environments but

many others had little or no controls in place, with new developments being coded and tested in the same environment as live systems.

Systems Development Controls	1 Does not exist	2 Poor	3 Part Only	4 Good	5 Active	Row Total %
Project Management	3.3	21.7	36.7	23.3	15.0	100
Development Team Composition	6.7	38.3	8.3	18.3	28.3	100
Development Methodology	6.7	25.0	16.7	25.0	26.7	100
Requirements Specification	35.0	23.3	18.3	10.0	13.3	100
System Documentation	30.0	30.0	16.7	10.0	13.3	100
Design Controls	36.7	36.7	5.0	13.3	8.3	100
Walkthroughs	15.0	28.3	10.0	16.7	30.0	100
Testing	31.7	23.3	26.7	6.7	11.7	100
Separate Environments	20.0	16.7	21.7	30.0	11.7	100

Table 5.5: Frequencies of Systems Development Controls (% of organisations surveyed)

The results of bivariate correlations of systems development controls with other variables was similar to the two areas of security measure implementation reported above. Significant relationships between systems development controls and corporate security measures were generally strong (see Appendix D.3). Active corporate measures generally occurred together with active systems development measures, and conversely where corporate measures were poor or absent, so were systems development measures.

Quality assurance is a corporate security variable which requires further investigation. As quality assurance methods and standards rely heavily upon the use of systems development controls, it is anticipated that a strong association would have been evident with bivariate correlations on these variable types. Each systems development variable did indicate a significant correlation with quality assurance. However, as quality assurance methods at a corporate level were absent in 75% of organisations studied, the crosstabulation tables for the systems development controls

invariably show a concentration of occurrences at the lower ratings of each pair of variables. A similar situation appears to be the case for an association between operational security measures and systems development controls, where the pattern of both implementation and lack of controls occurs. Each systems development control showed a remarkably consistent association with all other systems development controls. This suggests that an organisation using one type of control also uses the other controls studied, and conversely where some controls are absent or poorly implemented, others tend to be also absent.

Significant correlations (at the 0.05% level) of systems development variables with security problem variables occurred spasmodically and showed no apparent overall pattern.

5.4.4 Occurrence of Security Problems

A summary of the frequencies of security problems occurrence and impact can be seen in Table 5.6 below. The major problem areas appear to be lack of documentation; problems relating to data including errors, corruption and loss; denial of use due to hardware and software problems and unlicensed software. The least reported problems were fraud, hardware theft, software and data theft and sabotage.

There were no organisations that were free from any of the listed security problem areas. Errors in data were experienced by a large majority of organisations, and data corruption, loss of data and system downtime occurred in at least three-quarters of cases. At least one case of known fraud was experienced by more than one-quarter of the organisations, logical access violations occurred in more than half the organisations, and physical access violations in approximately four out of ten cases. Hardware, software and/or data theft and sabotage occurred in approximately one-quarter of firms studied. Rogue code (including viruses) occurred in some form in more than half of the organisations.

Significant relationships of controls with problems from statistical results are not readily obvious in practical application (see Appendix D.4). Some relationships link

with ease, for example logical access controls indicate a significant relationship with data integrity and availability problems (ie data corruption, data error, loss of data, denial of use) and logical access violations. The crosstabulations revealed that an absence of data integrity and availability problems occurs in the same environment as good implementation of logical access controls, and a tendency for these problems to occur where logical access controls are poor. The link between logical access controls and logical access violations is concentrated in one direction only, i.e. where logical access controls are in place and active there is an absence of logical access violations.

Security Problem	1 Major Problem	2	3	4	5 No Problem	Row Total %
Data Error	8.3	13.3	33.3	30.0	15.0	100
Data Corruption	8.3	11.7	20.0	35.0	25.0	100
Loss of Data	5.0	18.3	28.3	26.7	21.7	100
Denial of Use	8.3	11.7	23.3	33.3	23.3	100
Lack of Documentation	20.0	13.3	28.3	15.0	23.3	100
Fraud	6.7	8.3	6.7	5.0	73.3	100
Logical Access Violation	3.3	10.0	26.7	13.3	46.7	100
Physical Access Violation	6.7	5.0	20.0	10.0	58.3	100
Software, Data Theft	8.3	3.3	10.0	1.7	76.7	100
Hardware Theft	6.7	1.7	11.7	0.0	80.0	100
Sabotage	8.3	5.0	6.7	3.3	76.7	100
Unlicensed Software	18.3	1.7	11.7	10.0	58.3	100
Rogue Code	6.7	8.3	16.7	23.3	45.0	100

Table 5.6: Frequencies of Security Problems (% of organisations surveyed)

Bivariate correlations of security problem variables with other security problem variables resulted in consistent significance at the 0.05% level. Due to the low frequency of reported incidences over the range of security problems studied, crosstabulation tables generally show a concentration of occurrences in the cells

around the ratings of 4 and 5 for each variable pair studied (i.e. low or non-existence of security problems in the same environment). Expected significant links between security problems and the absence of related security measures were not reflected in these results, possibly due to the low occurrence of security problems. Based upon this sample, it is impossible, therefore, to suggest with any certainty that such links actually exist.

5.4.5 Factor Analyses

As is evident from the previous section a large number of variables were assessed as part of the corporate, operational and system development security measures and identified problems. As one would expect there are a number of associations between the specific measures in each category and with the various industry and organisational factors.

It was considered useful to use factor analysis to determine whether there existed summary "principal components" for each of the categories of corporate, operational and system development security measures and for the specific types of security problems.

Separate factor analyses were conducted for each category of security measure. These analyses were performed using the Factor analysis module of SPSS. Analyses were based on the correlation matrix the solution was un-rotated. Factor scores were saved as new variables for use in further bivariate and multivariate analyses.

The analyses extracted a single factor for each of the 3 categories of security measure (corporate, operational and system development) and two factors for the category of security problems. With respect to the latter the analysis clearly separated the problems associated with "illegal" behaviour (fraud, theft, sabotage, use of unlicensed software etc) from those associated with poor management of information (data error, loss and corruption, maintenance, documentation etc).

The resultant factor scores were used as the dependent variables in analyses (oneway ANOVA) which explored the relationship between type of security measure or problem and industry and organisational issues. In all cases the results obtained from these analyses were consistent with the crosstabulation and bivariate analyses reported below.

5.4.6 Qualitative Analysis of Security Measures and Problems

Qualitative analysis of interview notes and observations support the observations based on the frequencies noted above. Executives generally considered information security to be totally the domain of the auditors, security manager or IS staff. Commitment to the integrity, availability and confidentiality of information was commonly limited to those measures required to obtain a financial audit clearance. As one would expect, IS auditors displayed a greater awareness of security risks and preventative measures than IS and general management. In many cases written documents such as audit reports and minutes of meetings, detailed discussion and recommendations regarding the need for security measures, however, these were seldom actioned.

Security measures which related directly to the production of revenue or financial information systems received the greatest emphasis. It was also evident from discussions that many security measures had been implemented in response to human error, accidents or the occurrence of security breaches in their own organisation or firms with which they interacted.

The majority of managers agreed that security of information was an important issue, and should receive greater attention at all levels within the organisation. Many managers pleaded limited resources and time to dedicate to security issues. A lack of knowledge about security vulnerabilities and methods of minimising exposure was also admitted by nearly all participating senior managers.

Managers generally admitted they have no means of detecting security misuse, abuse or potential security problem areas. What to look for, where to look, or methods of

detection were not common knowledge amongst these managers. They also exhibited very little knowledge of legal requirements or methods of gathering evidence.

5.4.7 Industry and Other Organisational Factors

Frequency distributions and bivariate correlations were performed on industry and organisational variables and one-way ANOVA was used to examine the relationships between these variables and all types of security measures and problems. Appendix D.4 summarises the significant relationships found.

The most dominant industries in this sample were building and construction (13.3%), health and medical (13.3%), and retail and wholesale (13.3%), followed closely by State Government agencies (11.7%). The industries not represented by the sample were agriculture, automobile, conglomerates, education, food and beverage, insurance, publishing and communications, and textiles and footwear. The combination of State and Federal Government agencies totalled 16.7%.

The type of industry was found to have a significant correlation with nearly all corporate security measures and security problems, however, it showed little significance with operational and systems development measures. The distribution of occurrences for the implementation or absence of corporate security measures does not present any strong industry patterns. Similarly, no patterns emerge from the crosstabulation tables of industry type of security problem variables. However, the small number of cases in each industry group significantly limits the power of the statistical analyses.

Separate analyses were performed to compare self-reported security problems in the health industry with all other organisations grouped together. They showed a consistency of security problem occurrences in the Health and Medical industry which surpasses the other industries combined.

The type of software development and operations platform was predominantly third generation language (41.7%). Development tools and fourth generation languages were used by 35%, with the remaining 23.3% utilising packages or modified modules of software. One-way ANOVA of the factors representing security measures demonstrated significant associations between the type of software platform and most security measures. Security problems relating specifically to the integrity and availability of data also appeared to be significantly related. The type of software platform displayed a relationship with both maturity of users and centralisation. As users became more mature (in Gibson & Nolan's terms), there is a tendency to move from 3GL's to 4GL's. Highly centralised environments predominantly utilised 3GL software platforms and decentralised tended more towards 4GL than 3GL platforms.

With regard to span of impact on the organisation's operations, the majority of participants had systems which affected numerous sections or departments (56.7%). A small percentage (3.3%) had impact confined only to the immediate department, whereas 40% affected the entire organisation's activities if the system was not available or had questionable integrity.

One-way ANOVA tests showed little variation in security measure levels between different span of impact categories, i.e. span of impact had no effect on security measures. The results also indicate that the largest impact from security problems was where the span of impact was on numerous departments or the entire organisation.

Sensitivity of the data held on the systems studied was generally high, with 31.6% available only to selected individuals or a given department, and 45% being confined to a number of departments within the organisations. "Organisation only" restrictions applied to 13.3% and public access information was represented by 10% of organisations. This indicates that a total of 76.6% or organisations were dealing with information that needed to be restricted to certain sections or individuals only.

The sensitivity of data showed significant relationships with all security problems using ANOVA and bivariate correlation, however relationships with security

measures were not evident. Even with the low reporting rate of occurrences of security problems in the sample, organisations reporting highly sensitive systems (ratings 1 and 2) were generally found to have experienced security problems.

The majority of organisations were in the contagion phase of IS maturity (55%), with an emphasis on expanding computerised application areas. It is interesting to compare the number of organisations within the control phase with the level of security controls in place. The general lack of controls in and around information systems would support the 73.3% of organisations not yet addressing the control issues.

One-way ANOVA was performed on the maturity of users with security measures and security problems. Variations in the expected directions were apparent between user maturity and all systems development security measures, with additional variations with security measures at the corporate and operational levels. More mature organisations reported more active corporate, operational and system development security measures.

With regard to the size of systems, using the number of users as a guide, the highest rating category was 10-20 users (60%), with 23.3% in the 21-80 user bracket, and 16.7% having in excess of 80 users. The crosstabulation tables indicated that systems with smaller numbers of users tend to have less known incidences of problems. Systems with 20 or more users invariably experienced problems at higher levels, these problems having greater frequency and impact on the organisation.

The majority of organisations studied tended to have more centralised than decentralised computer hardware, software and data. Those organisations being highly or completely centralised totalled 61.7%, those with high or complete decentralisation totalled only 20%, and 18.3% were at least as centralised as they were decentralised.

Analyses showed that the extent of centralisation is significantly related to the majority of security measures, but not strongly related to security problems. Highly

centralised systems are notably poor in the implementation of security measures of all types, with improving security measure implementation ratings for more decentralised environments.

5.5 FINDINGS

The research theme that guided this study was ascertaining the level of action taken by management and users to ensure the integrity, confidentiality and availability of information. Each of the variables studied contributes to an overall view of the state of information security within organisations.

5.5.1 Current State of Information Security Management

The most prominent finding from this study is the general absence or poor implementation of widely recommended information security measures. This is indicated by the low frequencies of active security measures at the corporate, operational and systems development levels. In addition to the inadequate ratings shown by the quantitative analysis, qualitative analysis indicated the implementation of piecemeal solutions as a reaction to security problems rather than proactive, preventative security management.

As discussed earlier in this chapter, the process which precedes action involves an awareness regarding security issues and an acceptance of responsibility which then leads to a conscious decision to take action. The poor management of information security found in this study appears to be fed by a number of issues related to awareness.

5.5.1.1 Lack of Awareness

- a lack of awareness by management and staff of security risks and vulnerabilities
- a lack of awareness by management and staff of basic protective mechanisms and currently available security measures

- a lack of awareness of management procedures and tasks to ensure the ongoing integrity, confidentiality and availability of corporate information
- a lack of awareness of basic methods for the detection of misuse, abuse and errors leading to an inability to recognise actual and potential security problems
- a lack of knowledge of the legalities surrounding the protection of information and means of collecting evidence for prosecution, if required.

The results of this study clearly demonstrated that the level of awareness held by management and user staff regarding information security issues is generally low.

5.5.1.2 Poor Management Commitment

Commitment by senior management to information security is necessary to successfully ensure the integrity, confidentiality and availability of data. The level of this commitment is indicated by the implementation and active management of corporate security measures. Based upon the poor implementation of corporate security measures of the organisations in this sample, management's commitment to information security appears to be generally low.

5.5.1.3 Poor Responsibility Assignment

The direct management of information security and its active supervision, plus the distribution of responsibility for security to information authors, custodians and users, will indicate the level of acceptance of responsibility for the integrity, confidentiality and availability of information by staff and management. The majority of organisations studied displayed inadequate security management and supervision (ratings 1, 2 and 3). The allocation of responsibility for information security is apparent, however this appears to have been distributed to a level of employee with insufficient power and resources to supervise security effectively. The allocation of responsibility for information security to those staff members who are authors, custodians or users is remarkably low, with less than 12% achieving an adequate rating (rating 4 or 5).

It follows, therefore, that the commitment to, and acceptance of responsibility for, the integrity, confidentiality and availability of information by management and user staff is also low.

Hence it is possible that the lack of action could be the result of a general lack of awareness regarding security issues in addition to an absence of commitment and acceptance of responsibility for the security of corporate information. It must be acknowledged that there is no cause-effect relationship proven by this research, and this premise is not a result of testing a research hypothesis. However, the results do indicate significant associations that are consistent using a range of parametric and non-parametric bivariate and multivariate methods.

These results are consistent with the results from previous studies, discussed in Chapter 2, in particular that security awareness is low and the implementation of security measures is inadequate to ensure information integrity, confidentiality and availability.

5.5.1.4 Other Findings

Other findings not directly related to the research theme also emerged from this study.

Security education is not widely undertaken within the organisations studied. According to the Macquarie Encyclopedic Dictionary, 'education' is *the imparting or acquisition of knowledge* (page 294), and 'knowledge' is *the state of being cognisant or aware* (page 519). It would follow, therefore, that education about information security risks and protective measures would provide knowledge and engender a greater state of awareness regarding security issues. With a greater awareness of security risks and possible security measures to minimise those risks, management and staff are in a better position to decide the extent to which an asset needs protection, the most appropriate measures to implement, and the priority with which it should be handled.

Correlations between the implementation of security measures and the known occurrence of security problems occur erratically. It would appear from the data collected that the absence of, or poor implementation of, particular security measures occurs in the same environments as the absence of security problems. Similarly the existence of active security measures occur in the same environments as frequent or high impact security problems. This could indicate that either:

- the general belief that active security measures minimise the occurrence of security problems, and security problems occur in environments with poor security measures, is ill-founded, and/or
- security problems are occurring in environments with poorly implemented controls, however, managers are not aware of these problems.

The majority of participating organisations had not reached the 'control' stage of IS maturity. This is supported by the general lack of security measures implemented by organisations in the 'initiation' and 'contagion' stages of maturity. Security measures for organisations in the 'control' and 'maturity' stages were notably higher in rating.

A large number of managers admitted a lack of knowledge of detective mechanisms that would uncover security problems within their organisations. It is possible, therefore, that the data collected on security problem areas does not reflect the true situation. With little or no methods of detection, it is unlikely that managers are able to present an accurate picture, whether that picture be positive or negative.

Participating managers in general considered information security to be a technical area. When asked to explain what they understood by the term 'information security', managers almost exclusively spoke of encryption, firewalls on networks, passwords, digital signatures and smart cards. The role of *people* in the securing of corporate information was seldom recognised.

Security measures were considered overheads to system and user performance. Additional controls were assumed to slow computer systems down, increase delays in access time, and be costly in nature. Very few managers had investigated current

products and prices of basic security measures. In addition, security was viewed as a policing role where rules or laws needed to be established. It was generally assumed that additional staff would be required to 'police' these rules.

The aims of integrity, confidentiality and availability of information were rarely considered to be part of information security with many managers regarding these requirements as part of a quality management program. Hence we see a lack of awareness of the scope of information security at a core level within organisations.

5.5.2 Needs Arising from Findings

There are a number of factors for management consideration arising as a result of this study. The absence of organisation-wide security measures implies that effective management practices are not in place. In order to change this situation, the following factors should be considered.

Organisations need to employ methods encouraging a wider and more comprehensive view of security. A holistic view of security which views information as a corporate asset for the total organisation is required. Planning for security, based upon corporate policies and organisational goals will ensure the 'big picture' is addressed. This would minimise the current trend to implement piecemeal solutions which do not work efficiently together, and minimise security measures in competition with one another. Corporate-wide considerations of risks and security measures would result in a comprehensive and integrated approach, and also ensure consistency of standards throughout the entire organisation.

A proactive stance toward managing information security, using preventative rather than reactionary methods would also assist. Knowledge of risks and areas of vulnerability will aid in determining the most effective protective measures and where they should be applied. Senior management recognition of the need for information security and commitment to achieving it is essential.

Security needs to be mission-driven to ensure that security measures support and complement organisational objectives. Compliance with organisational aims will help in determining appropriate security measures and their level of importance. This involves not only being aware of organisational goals and missions, but also how information helps to achieve those goals. The information most crucial to reaching those goals should form the highest priority for implementation of protective measures.

There is a need to build a security culture within the organisation, engendering automatic considerations of security issues in the mind-set of all employees. Security considerations then become part of everyday work operations and planning activities. A necessary part of a security culture will be the security education program. The raising of security awareness through education programs for staff at all levels, will increase the ability to recognise risks and vulnerabilities and integrate appropriate solutions.

5.6 LIMITATIONS

The population size of sixty organisations participating in this study could be seen as inadequate to produce generalisable findings from the statistical analysis. Presenting generalisable findings was not the aim of the research, however, and the sample presented is believed by the researcher to be of sufficient size to give an indication of the state of information security in Australian business organisations.

The chosen sample of organisations could be biased. The participating organisations were drawn from a pool restricted to two main sources; organisations sending attendees to professional development courses, and organisations providing sites for computer projects at undergraduate and postgraduate levels. The organisations were required to fulfil the criteria discussed earlier in this chapter, and the sensitivity of the investigations carried out at each site resulted in a high proportion of the organisations originally approached declining to participate in the study.

It cannot be assumed that any relationship between security measures and security problems are cause and effect. This research did not study the level of occurrence of security problems before and after the implementation of given security measures. It cannot be said that a given problem will decrease with the implementation of a particular security measure or increase with the removal of a security measure. This cause-effect notion was not part of the study. The only relationship that can be implied from this study is that given security measures and security problems may occur in the same environment.

In any study involving interviewing and observation, there is always the risk of bias of the data gatherer. The interpretation of the spoken word by the interviewer can be different to the meaning or essence projected by the interviewee. The interviewer can also be seeking certain patterns or inferences to support ideas or research questions. This study involved the interview of more than one staff member at each site, and different interviewees may interpret questions differently. The ratings of security measures and problems assisted in the interpretation of information and provided a framework for categorisation of the data collected. The ability to interview a number of different personnel and access written documentation was also an advantage, as triangulation via different sources was able to be carried out to verify the information given by any one party.

Despite the limitations of the study, the remarkable consistency of the observations using a range of methods, and the similarity of the observations with those reported in the literature suggests that the key observations are robust.

5.7 CHAPTER CONCLUSION

A study of the current security practices for sixty Australian organisations has been described. The aim of the study was to build a picture of information security within the organisations, giving indications of the level of awareness regarding information security issues, the commitment to and the acceptance of responsibility for information security, and the level of action taken to ensure the integrity, confidentiality and availability of information within the organisation. The study

collected data on the implementation of security measures and occurrence of security problems within those organisations.

The qualitative and quantitative analysis generated results which indicate that security measures are generally poorly implemented and managed within the organisations studied. The conclusions reached are that the level of awareness of information security is low; the commitment to, and responsibility for, information security is low, and the level of action to ensure the security of information is also low.

Due to the general lack of planning and active management of information security evident in the organisations studied using current management methods, there appears to be a need for an alternative approach to information security management. This alternate approach needs to consider a holistic view of security, integrating security planning with organisational missions and goals. Security education programmes for all levels of staff would aid in the building of a security culture and encourage a raised awareness of security issues and acceptance of responsibility for security measures. Such an approach would meet the current shortcomings of information security management, in particular the implementation of piecemeal security solutions in response to security problems or violations.

6. THE ORION STRATEGY

6.1 CHAPTER INTRODUCTION

The review of literature relating to the current state of information security management and available models for information security planning and management highlighted the need for more appropriate security management approaches. In particular, the need for raised awareness of security issues and ownership of responsibility for security is evident. This chapter presents an approach that combines high user involvement with a problem solving methodology encompassing a paradigm change in thinking, in an effort to improve information security management. The problem solving approach used as a base is the Soft Systems Methodology (SSM) originally devised by Checkland in 1981, and its application to security and risk management has been previously suggested (Baskerville 1988; Baskerville and Wood-Harper 1996; Lane 1985). The aim of using SSM in this situation is to increase stakeholder commitment to the secure management of information. The early part of this chapter explains the Soft Systems Methodology (SSM) and how it was used to build the Orion Strategy, an alternative to the current security planning and management approaches. A detailed description of the Orion Strategy then follows.

6.2 CHECKLAND'S SOFT SYSTEMS METHODOLOGY

SSM, a soft systems approach to problem solving, was first introduced by Checkland (1981) as a methodology for tackling problematic situations. This methodology uses both *systems thinking* (or modelling of an ideal situation) and *real world thinking* (modelling of the real world situation) by the people directly involved in the situation under study. This methodology "is a means of guiding the tackling of real world situations which are perceived as problematical for some of the time by at least one member of that situation" (Davies and Ledington 1991, p11). SSM was developed in response to the inadequacy of systems engineering approaches to situations where objectives are complex and poorly defined, and where differences of opinion are numerous.

Most 'real world' management problems are characterised by obscurity and complexity, in contrast to ideal or academic situations where human considerations are held constant or not included. SSM has an emphasis on human activity systems, comparing ideal or conceptual thinking in the systems world with what is currently occurring in the real world. The gaps are then analysed and solutions that are considered feasible and desirable are implemented. One of the most important aspects of SSM is that the people most directly involved with the problem situation carry out the problem analysis in practice. It is, in effect, handing over the problem analysis and desired action to those persons who have a stakeholding in the problem situation.

The soft systems methodology is illustrated in Figure 6.1. A revised diagram illustrating the methodology was devised later (Checkland and Scholes 1990). The methodology itself remained unchanged, however, the diagrammatical format was altered and presented in a more pictorial form. In order to appreciate how the methodology has been adapted to this and other research situations (see 6.3 Applications of SSM and Appendix E) it has been necessary to use the original version from Checkland (1981) in this thesis.

Activities 1 and 2 seek to build the richest possible picture of the problem situation, in all its complexity and according to the various perceptions of the stakeholders. The main technique used is the 'Rich Picture', a pictorial representation illustrating the current situation and any perceived problems. Users are encouraged to undertake an analysis of the problem situation in the real world and identify systems that are relevant to the discussion. By debate, those involved directly in the functioning of these systems hope to unearth ways to alleviate or solve the given problem situation.

Activities 3 and 4 build models of the activities relevant to the problem situation, taking into account the organisation's goals and future, aiming at an ideal solution to the inadequacies of the present day.

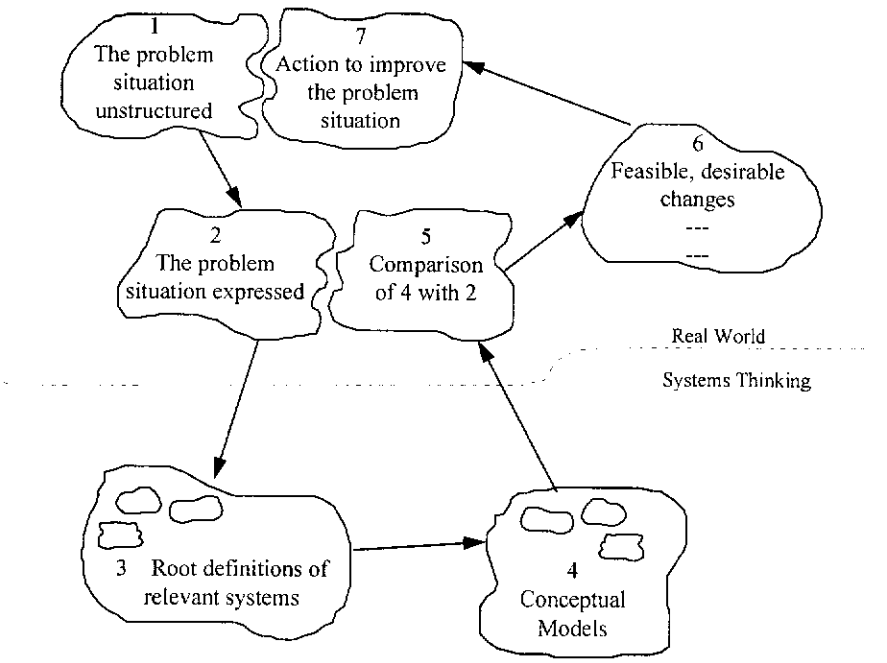

Figure 6.1 Soft Systems Methodology Source: Checkland 1981, p163

The models are then compared with the problem situation (activity 5), participants being encouraged to debate the differences and identify means by which improvements may be made. Strong reality-checking takes place in activity 6, to ensure that proposed actions emerging from the process are both practically feasible and culturally desirable in their implied effect. The final activity involves developing an action plan and implementing the finally agreed solutions.

These seven activities are not necessarily followed in a sequential order and the method incorporates the ability to return to earlier activities at any stage. This need may be frequent in unstable, dynamic or complex situations under study. In particular, a revisiting of earlier stages may be necessary where there is continuing uncertainty or ambiguity at any stage (Dick 1993).

The systems identified as 'relevant' in the early activities of the methodology are principally referred to as human activity systems. These systems are not physical systems (such as departments, computerised information systems or the like) but

systems (in the widest sense of the word) which are comprised of related groups of activities carried out by humans. A human activity system within SSM is a particular kind of holon; where a holon is defined as a constructed abstract whole system, i.e. "a set of activities connected so as to make a purposeful whole, constructed to meet the requirement of the core system image (possessing emergent properties, layered structure, processes of communication and control)" (Checkland and Scholes 1990, p26).

As there are usually numerous stakeholders in a given problem situation, there will be different perspectives held by each, depending on the stake involved. SSM caters for numerous views of the given situation, and encourages debate and discussion in an effort to reach a common understanding of the essential issues. "In examining real-world situation characterised by purposeful action, there will never be only one relevant holon, given the human ability to interpret the world in different ways. It is necessary to create several models of human activity systems and to debate and so learn their relevance to real life" (Checkland and Scholes 1990, p27). This is particularly the case when dealing with information systems and information security, as there are many different parties who are stakeholders in such systems.

6.2.1 Altered States of Thinking

The secret of real success in the move from the real world to the conceptual world is the ability of the participants to put aside concerns of the current situation and focus solely on a desired perfect scenario which achieves all the stated goals and objectives of the given human activity systems. One of the key strengths of SSM is the move from one state of thinking to another, whilst keeping the first state on hold. This is akin to working in a windowed computing environment. Work commences on the problem situation in the real world state and then a new window representing the ideal or conceptual world is opened. Following an in-depth analysis or working of this ideal state, the current situation window is reactivated and compared with the ideal. These states are referred to as *dialectics* (Dick 1993) and SSM may be described as a non-numerical systems approach to diagnosis and intervention. Dick analyses the method using dialectics as illustrated in Figure 6.2.

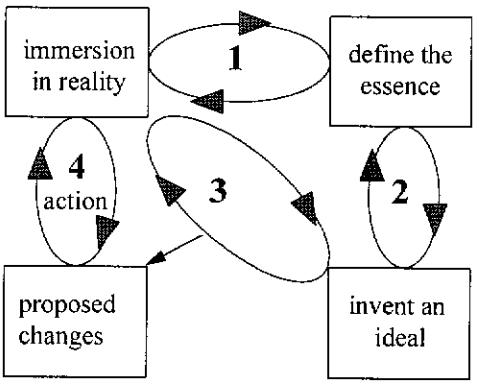

Figure 6.2 Dialectics of SSM (source: Dick 1993, p23)

The first dialectic is where one immerses oneself in the reality, to try to capture the essence of the system in a description, usually in terms of its most important functions. The second dialectic is between the description of the essence and a depiction of an ideal, where working from the description of the essential functions, an ideal system is devised. The third dialectic is between the ideal and reality, comparing the ideal to the actual system, noting any differences. This gives rise to proposals for improvement to the reality which in turn leads to action, the fourth dialectic. The process of action leads back to an immersion in reality where the changes are physically implemented.

6.2.2 Tools of SSM

The tools commonly used in the implementation of Checkland's traditional SSM are rich pictures in activity 2, root definitions in activity 3, and conceptual models in activity 4. Regardless of the type of implementation these tools appear to be used in most applications of the methodology.

6.2.2.1 Rich Pictures

This method of illustration is a form of analysis, allowing the participant to express the situation as they perceive it in a simple picture. A picture, in general terms, is a universal communications language, allowing expression of feelings and perceptions to be made manifest in a concrete form. "There is no formal technique or classic form for this, and skill in drawing is by no means essential (though it's not a hindrance!) in the production of pictures which are found to be very helpful." (Checkland and Scholes 1990, p45).

Prose may be particularly bad at conveying relationships within systems thinking and it helps to clarify the thinking about a situation when illustrated through a picture (Wilson, 1991). Rich pictures "express in a condensed way relationships which would require much prose to expound" (Checkland and Scholes 1990, p45). The rich picture may be used to express the problem situation by condensing the information that has been gathered (Davies and Ledington 1991, pp20,21). The rich picture could thus be defined as an expression of the problem situation and the relationships therein in pictorial form developed by condensing information that has been gathered from a number of sources. Figure 6.3 contains an example rich picture for paramedical services of a health district.

Rich pictures are an individualistic expression (Davies and Ledington 1991; Patching 1990) and there are no hard and fast rules in their development and use. The interpretation of a picture can be different for each viewer. A picture may be interpreted quite differently by one reader, and more can be read into the picture than physically meets the eye. Many political undertones, unspoken fears, concerns and desires are hidden within a picture. The term 'rich' picture is quite an appropriate label for these illustrations as there is a rich pattern woven into the tapestry on paper. In many cases words cannot fully explain the tapestry seen by individuals involved in a particular situation. The drawing of a picture can build a scenario of the 'truth' as it is perceived by that individual for others to contemplate. In addition to clarifying each

person's 'truth', rich pictures are also a means for individuals to express their feelings about a given situation without having to find acceptable and non-threatening words.

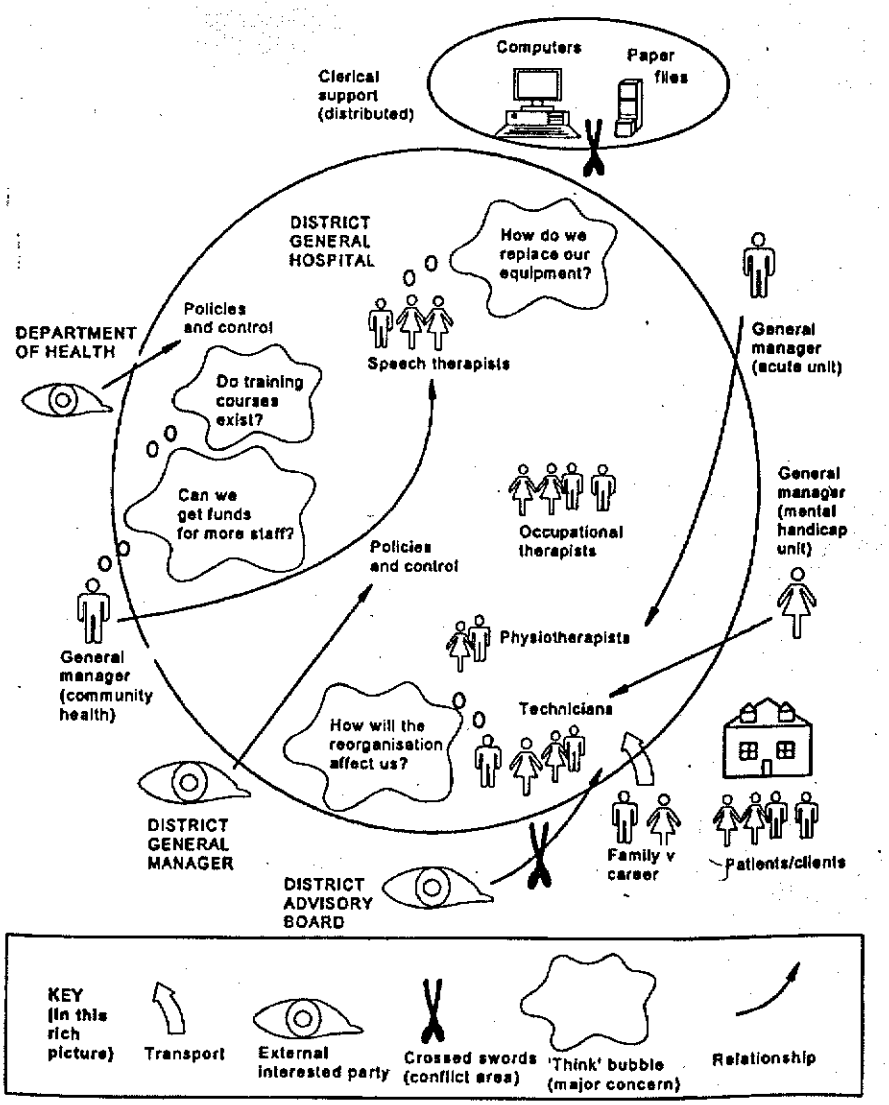

Figure 6.3 An Example Rich Picture for Paramedical Services of a Health District Source: Avison and Fitzgerald 1995, p369

Participants are encouraged to use rich pictures to illustrate the current situation of the organisation, for several reasons. Firstly, illustrating a situation in picture form does not allow participants to slip into a habitual verbal mode, where well-rehearsed position statements are delivered without any serious reflection upon them. Secondly, it forces participants to confront what they believe the situation is like. Thirdly, it allows participants to produce radical statements which could be quite critical of the status quo and colleagues, in a mode which is relatively non-threatening and unlikely to give offence, "after all we are only drawing pictures and playing games" (Jones 1991, p167).

The compilation of rich pictures from a number of participants builds a much broader and detailed picture of the total situation. Similar themes often emerge as participants illustrate parallel thinking, and quite opposite views can also be found as the combined picture takes form. Once the rich pictures have been produced they serve to stimulate joint critical reflection upon what the implications of those pictures are for the department, its organisation, its goals, its procedures and the interaction of the people within them (Jones 1991).

The rich picture has become an integral part of SSM. Rich pictures are considered appropriate because human affairs reveal a rich moving pageant of relationships, and pictures are a better means of recording relationships and connections than linear prose. Rich pictures are used extensively in the literature to illustrate concepts being explained. "A characteristic of fluent users of SSM is that they will be observed throughout the work drawing pictures and diagrams as well as taking notes and writing prose" (Checkland and Scholes 1990, p45).

6.2.2.2 Root Definitions

The aim of the two activities within the conceptual world of thinking is to define and model the essence of the ideal situation. "The ideal is derived from the essence, to reduce contamination by the way the system actually behaves .... the essence becomes the necessary functions" (Dick 1993, p25) and these are the 'root definitions'. A root definition defines a system at a high level recognising the stakeholders involved, the

purposeful action or reason the system is active, the world view and the environment in which the system exists and operates. Root definitions are formulated by considering elements comprising the following CATWOE mnemonic:

C	'customers'	the victims or beneficiaries of T
A	'actors'	those who would do T
T	'transformation process'	the conversion of input to output
W	'weltanschauung'	the worldview which makes this T meaningful in context
O	'owner(s)'	those who could stop T
E	'environmental constraints'	elements outside the system which it takes as given

(see Checkland and Scholes 1990, p35).

A root definition is then built from the CATWOE using the following as a guide: Checkland (1981, p317)

> A (...**O**...) owned system which, under the following environmental constraints which it takes as given: (...**E**...), transforms this input (...) into this output (...) by means of the following major activities among others: (...**T**...), the transformation being carried out by these actors: (...**A**...) and directly affecting the following beneficiaries and/or victims (...**C**...). The world-image which makes this transformation meaningful contains at least the following elements among others: (...**W**...).

This process is carried out for all identified 'sub-systems' of the high level system. The root definitions for each sub-system form the core of the conceptual models developed in the next stage of the methodology.

6.2.2.3 Conceptual Models

Conceptual models are an expansion of the root definitions into detailed theoretical models of the ideal holons or systems identified. "The system can be modelled as a whole entity in terms of an interconnected set of activities" (Wilson 1990, p53).

These models are a representation of the necessary activities each system or holon must do in order to be the system defined in the root definition. The activities forming a system are labelled using verbs, denoting the action to take place within each activity. Just as components of a system are interrelated conceptual models also show how activities are related to one another, illustrated by the positioning of each activity and its flows to and from other activities.

Conceptual models within SSM can be used as an aid to clarify thinking about an area of concern; as an illustration of a concept; and as an aid to defining structure and logic, and are a prerequisite to design (Wilson 1990). As emphasised by numerous users of SSM conceptual models are an expression of the ideal situation, and not a representation of the current situation. The development of these models is a more abstract process than that normally experienced in the derivation of descriptive models (Davies and Ledington 1991). The purpose of moving into an abstract world of thinking is to develop an alternate view of the situation, and once this has been developed it can be tested back in the real world. In effect, the conceptual model 'illustrates what aught to be happening to achieve the objectives specified in the root definition', (Avison and Fitzgerald 1995, p126).

6.3 APPLICATIONS OF SSM

Since its development SSM has been used as the base methodology for many studies in differing disciplines. SSM is a pure methodology, and "like methodology in general, it needs to be tailored to fit the nature of the enterprise in which it is to be used" (Wilson 1990, p197). A few examples illustrating the extent of its application in different situations are presented in Appendix E.

The flexibility of SSM allows it to be adapted to a given situation. SSM has had wide application in the information systems, organisational design and management areas. One of the main reasons for the success of SSM in these areas appears to be its human orientation.

6.4 FORMULATION OF THE ORION STRATEGY

The Orion model for information security planning and management is presented as an alternative to the highly structured traditional approaches. This approach shifts the focus of ensuring security away from the highly structured, complex and technical methods that rely predominantly upon security specialists, towards an environment where users are aware of security issues, understand why controls need to be put into place, and feel personally responsible for the security of information in their work area. Security planning and management functions are not performed as separate and specialist functions, but are integrated into mainstream planning and management and form part of basic organisational considerations. This ensures a holistic view of information security including assets, risks, and responses to threats, and builds both a corporate and personal ownership of security responsibility.

In such a scenario the security expert no longer dictates the protective measures to be implemented within the work environment, but acts as an adviser to users and management. In this way the organisation's employees are able to decide, with guidance from the security specialist, the most appropriate protective measures and fully understand the impact these will have on the work environment. This reduces the possibility of highly complex and technical security solutions being implemented and then scrapped by users due to the highly restrictive nature or inappropriateness of the measures.

Staff members working with the system are usually the first to identify security loopholes existing in the procedures and systems. Not only do the users and managers know more about the general operations of their systems and how they integrate, but they also know where the weaknesses are. Users are, in many cases, also aware of how these holes can be secured with a minimum of cost and effort. It is important, therefore, that users be consulted in the planning and management processes.

Traditional methods have concentrated on the technical and risk attributes of information security without due regard to the human, social and organisational elements. The Orion Strategy attempts to address these considerations, by a

combination of its application process as well as content via the basic set of activities. The method itself studies in detail both the current security situation and an ideal security position, noting where gaps between the two exist. Appropriate measures to fill these gaps are recommended and as protective measures are integrated into the work environment, so security is integrated into the organisational mindset. Security is not considered as a separate activity, but a necessary part of all organisational activities. User participation and human interaction are key features of the processes encompassed within this method.

Extensive user participation gives two distinct advantages. The first is the opportunity to tap into the extensive body of knowledge held by people who work in the organisation. Staff members know the daily operations and processes in great detail, and understand how they integrate together to achieve business goals. Technical experts may be knowledgeable in their own field of speciality, however, they cannot be expected to know the business operations of the organisation to the same depth or as widely as a body of employees will. The second advantage is the rise in profile of security issues as employees become involved in considering risks and possible protective means to minimise vulnerabilities in the work environment. Not only do users become more aware of security issues in general, but they also feel they can contribute to the solution and are therefore more accepting of necessary security measures implemented. A feeling of ownership of security solutions should be generated where employees have participated in the planning, design and implementation of such measures, recognising their necessity and origin. One of the keys to the success of the Orion approach is the marrying of people with information security and organisational expertise to build a holistic consciousness integrated into the organisational mind-set.

The first version of the Orion Strategy maps security activities directly to SSM activities. A high level interpretation of the Orion Strategy appears in Figure 6.4. This diagram shows the major phases, or activities involved in the method. As with SSM the Orion Strategy also has two planes of reality or conceptualisation. The first plane is the physical or real world where actions and processes can be seen, heard and measured - aspects which are concrete and scientifically provable. The second plane

is the abstract, conceptual or ideal level where situations and processes are imagined, and/or visualised, and scenarios built at an abstract, rather than physical level. This allows participants to consider aspects beyond the confines of physical reality, thus encouraging creativity.

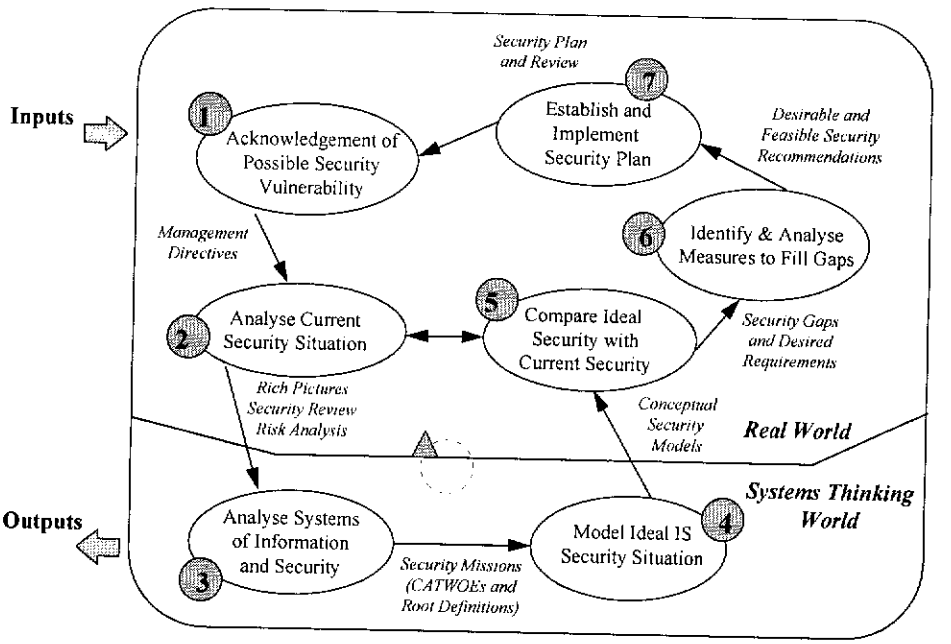

Figure 6.4: Orion Strategy - Highest Level

Activities are denoted by oval shapes in the diagram, and the arrows indicate inputs and outputs to and from these activities. There is a boundary line encompassing the main activities, separating the area under consideration (usually the organisation itself or the section under study) from external influences. For example, inputs could include legal and statutory requirements; directives from boards of directors; strategic, organisational and human factors; or inflows from other bodies or systems. Examples of outputs would be defined security requirements, action plans and reporting to management. These influences can flow through the boundary to affect any of the activities within. The approach contains seven main activities and these are numbered for guidance only. Although the sequence is logical there is no hard and fast rule that activities need to be followed in the sequence of their numbering. In many cases it is

necessary to go back and revisit past activities as the environment changes and new influences take effect.

The New Hamlyn Dictionary (1988, p1654) defines a strategy as "skilful management in getting the better of an adversary or attaining an end", also "the method of conducting operations, especially by the aid of manoeuvring or stratagem (a plan or scheme)". Methodology is defined as "the science of method" (New Hamlyn Dictionary 1988, p1052). As this research is particularly interested in the practical application of an organised set of activities forming a plan for a course of action, the term strategy is used in preference to methodology.

6.4.1 High Level Orion Strategy

The Orion Strategy in Figure 6.4 illustrates how SSM can be projected into a practical information security planning and management environment. Security was viewed as a separate system within the organisation at this point in the research. Practical application of the approach would indicate any modifications subsequently required to assumptions, activities or premises (see the next chapter for the changes made during the application of the model).

The first two stages of SSM are expression phases "during which an attempt is made to build up the richest possible picture, not of 'the problem' but of the situation in which there is perceived to be a problem" (Checkland 1981, p163). A particular structure should be avoided in the building of this picture, and that slow-to-change structures be studied with relation to continuously changing processes within the situation under consideration. The function of stages 1 and 2 is to display the situation so that a range of possible and relevant alternatives can be identified, and that is the only function of those stages. (Checkland 1981)

The first SSM activity was *The Problem Situation: Unstructured*, and this equates to *Acknowledgement of Possible Security Vulnerability* in the Orion model. This SSM phase is characterised by a collection of as many perceptions of the problem situation as possible without using analysis in systems terms, and selection of a particular view

for continued study. In the Orion model, information and perceptions of security vulnerability are gathered from different sources and management becomes aware that a potential problem exists.

Activity two in SSM *is The Problem Situation: Expressed*, which is mapped to *Identify Risks and Current Security Situation* in the Orion model. A more detailed picture of the current situation is drawn up in this stage using SSM, emphasising the importance of 'structure' and 'process' in this context. Here structure may be examined in terms of physical layout, power hierarchy, reporting structure, and the pattern of communications both formal and informal. Process is looked at in terms of the basic activities of deciding to do something, doing it, monitoring both how well it is done and its external effects, and taking appropriate corrective action. (Checkland 1981, p166). This stage in the Orion model looks at both structure and process, and produces outputs in the form of rich pictures, security review reports and risk analyses which describe the current situation with regard to both process and structure. The monitoring and corrective action segments integrate with the overall monitor and control activity at the top of the Orion model (see Figure 6.4)

Moving down into the systems thinking world, activity three in SSM is *Root Definitions of Relevant Systems*, correlating to *Identify Ideal Security Situation for Information Systems* in the Orion approach. In SSM this is the phase where root definitions are developed, that is, "hypotheses concerning the eventual improvement of the problem situation by means of implemented changes which seem to both systems analyst and problem owners to be likely to be both 'feasible' and 'desirable'." (Checkland 1981, p167). This equates in the Orion model to a high level definition of 'systems' of information and the security attached to those systems. A 'system' of information here may not necessarily be represented by a computerised information system, as most systems of information have a human (as opposed to robotic or mechanised) element and associated manual processes. Both SSM and Orion Strategy activities take place in the ideal world, rather than the real world, and here the emphasis is not on current systems and current practices, but on conceptual and ideal systems, where all organisational, human, social and technical objectives are being met.

Activity four, *Conceptual Models* in SSM matches with *Model Ideal Information Systems Security Situation*; also in the conceptual world. This phase is to model the activities needed to achieve the transformation described in the root definition, and the activities together with their sequence, that have to occur in order to effect this transformation. "The definition is an account of what the system is; the conceptual model is an account of the activities which the system must do in order to be the systems named in the definition" (Checkland 1981, p169). In the Orion model, the systems of information are analysed and important characteristics and activities regarding each is devised in order that the ideal systems and their security features match the ideal definitions developed in the previous phase.

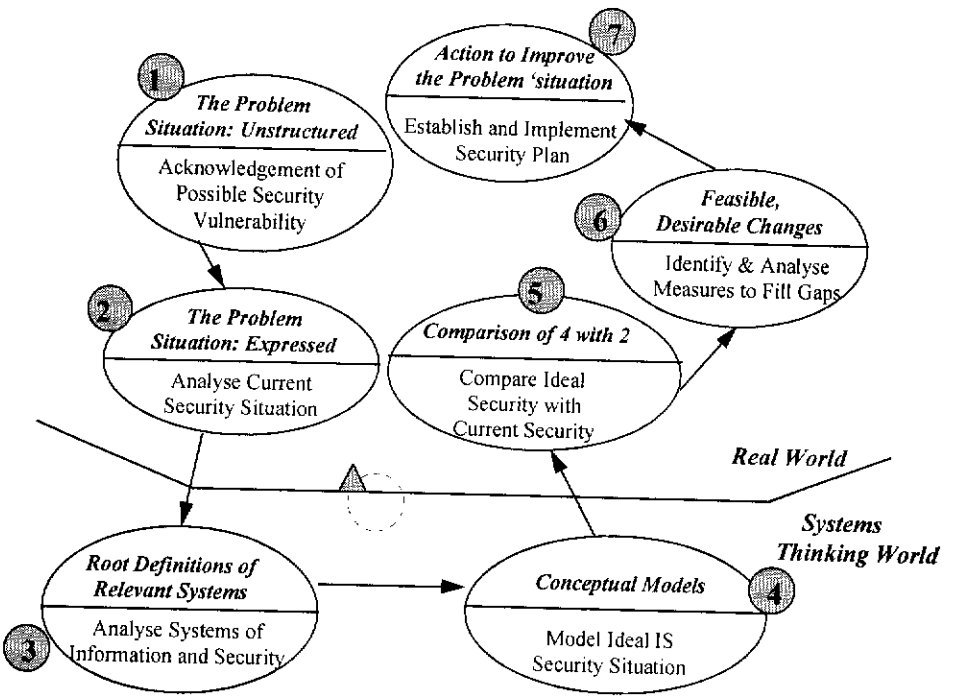

Figure 6.5: ***SSM mapped to Orion***

Taking these conceptual models back into the real world is illustrated in SSM by activity five *Comparison of Activities Four and Two*, and in the Orion model *by*

The cyclical nature of the approach means it is designed to operate in repetitive and ongoing motions. Planning takes place, then action puts the plans into effect, followed by review and reflection of the consequences, feeding back into further planning again. The activities do not necessarily have to be followed in sequence and it may be appropriate to revisit previous activities as planning progresses in order to incorporate changing factors. The iterative nature and action learning motion is an important part of the method, particularly as information systems and organisations are not static, but continually evolving and dynamic, and such an approach is the crux of learning and the learning organisation (see Bawden and Zuber-Skerritt 1991; Kemmis and McTaggart 1988; Thomas and Harri-Augstein 1991).

SSM was used as a basic framework for the application of information security planning and management for a number of reasons:

- SSM is an internationally recognised methodology and has been used extensively in a wide range of research spanning different disciplines.
- SSM is a flexible theoretical methodology designed to be adapted to the situation under study.
- The extensive involvement of stakeholders aims to both raise their awareness of security issues and engender a greater ownership of security measures and responsibility for their operation.
- The shift of analysis from the real world to the systems thinking world and back again for comparison is aligned to a paradigm shift as the thinking mode changes. The move into conceptual thinking is important because the participants transfer from dwelling on current physical occurrences to abstract and idealistic scenarios in the search for potential solutions or enhancement opportunities. Analysis of the current situation tends to be isolated and fragmentary in nature, and alludes to the source of the problems rather than identifying the problems themselves. In effect, systems thinking lifts the analysis to a more expansive and holistic level, viewing systems as holons rather than segmented sets of physical activities.
- Organisational factors can be easily recognised and accommodated in the planning and management processes. Strategic objectives are an essential input, and

organisational structure, politics, policies and management styles become key factors for consideration due to their influence on activities and possible outcomes.

- External influences and constraints are identified and their effects taken into consideration within solution planning. This means that consideration is expanded beyond purely internal factors and a much broader and realistic picture can be built of the current and ideal situations.
- Rich pictures are an integral part of SSM, and form a communications medium that is abstract and non-threatening to the majority of participants.

User participation is a necessary part of SSM in order to acknowledge the different perceptions of the parties who are stakeholders in the problem situation. The perceptions or views of each stakeholder will be centred upon the values and norms associated with their role. Each participant's view is based upon language and concepts relating directly to their perception of the situation, and of course, these will differ between participants. It is important, therefore, that a means of non-threatening and universally understood communications is established and used in order to appreciate the different views of the participants involved in the problem identification exercise. This is where rich pictures have been used as part of SSM in the past.

Rich pictures have been used in the design of the Orion Strategy, both as an activity within the method and as a means of expressing the process of carrying out the activities involved. The following section explains the Orion Strategy in detail and illustrates each phase using conventional symbols.

6.4.2 Orion Strategy in Detail

6.4.2.1 Phase 1: Acknowledgment of Possible Security Vulnerability

The first stage of the Orion approach is the recognition of possible vulnerabilities with regard to information security. This awareness could come through one or more source, such as press reports and media coverage of computer related abuse, indications of lack of integrity of information via questionable reports or corrupt data,

security breaches from within the organisation, informal channels of distributing confidential information, unreliability of systems and system down-time, and like circumstances. Figure 6.6 illustrates this acknowledgement phase.

One of the key issues is that the organisation's vulnerability is recognised by senior management, and a decision to take action is made by an executive with the power to enforce such a decision. It is also very important that executive management fully support such a move, for without support from the highest level, the security improvement exercise will not be fully successful. Once a decision is made to take action, a manager with the knowledge and authority to carry the responsibility of a security review and improvement project needs to be appointed by senior management. The output of this stage is a management directive regarding improving information security issued by executive management.

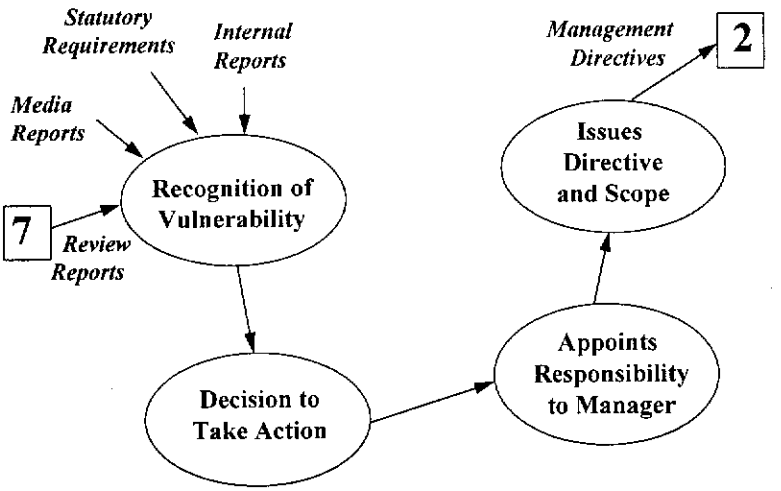

Figure 6.6: Phase 1: Acknowledgment of Security Vulnerability

6.4.2.2. Phase 2: Analyse Current Security Situation

The second phase of the strategy is to investigate and define the current situation with regard to information security within the organisation or section under study. This

phase involves *staff briefings* and compiling a big picture of the present situation via *security reviews*, *risk analysis* and *problem analysis* using rich pictures.

The first step is to *brief staff* on the management directive emerging from the previous phase, so employees understand and support the intentions of senior management. It is important that staff are aware of the actions that will take place and that their participation is essential to the success of the venture. A security specialist presents an awareness seminar to staff giving details of current trends in abuse and misuse of information, and the risks inherent in contemporary information systems. This education session is designed to improve the staff knowledge about possible risk areas and how abuse can occur. They are then encouraged to apply the principles to their own working environment.

During the *problem analysis* activity a picture of the current security situation is then drawn up by the staff in the form of a rich picture highlighting possible problem situations. These illustrative pictures are useful tools for a number of reasons including the non-technical nature of the problem analysis and the format that is easy drawn by a group of people, who do not have to be artistically talented. The rich pictures are an illustrative interpretation of current problem and potential problem areas, whereas the risk analysis is a more detailed investigation of specific risk areas, rather than problems currently occurring.

The manager assigned responsibility for information security would then activate a *security review*, to be carried out by an independent security specialist. It is important that such a review is not carried out by internal staff, as an objective and comprehensive review is required. This minimises any risk of internal manipulation or misrepresentation from parties with possible vested interests in the outcome. This review needs to be an in-depth investigation of current security procedures and measures and their effectiveness, and should cover all aspects of recommended security referred to in Appendix A. The end product of this exercise would be a security report submitted to management for collation with other information gathered from different methods.

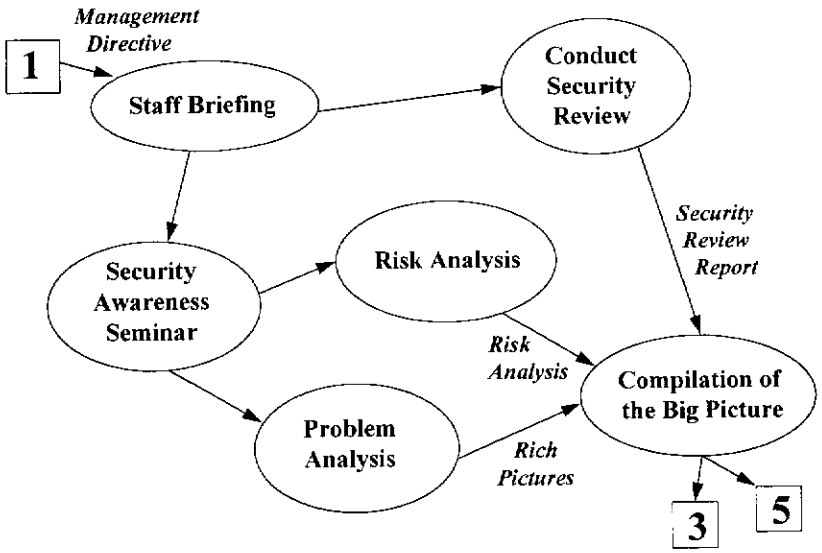

Figure 6.7: Phase 2: Analyse Current Security Situation

Risk analysis workshops are held with staff to identify particular risk areas within the organisation as a whole as well as in particular sections or processes. It is desirable that these workshops be conducted by an independent facilitator with management and security expertise in order to obtain an in-depth and objective synopsis of current risk areas. These workshops need to address the assets at risk and the threats that could affect these assets. Such analysis would usually mean that assets must be first identified and possibly categorised, and then associated threats identified and assimilated.

The risk analysis carried out is not necessarily a quantitative exercise, utilising complex mathematical formula, however, this can form a part of the analysis if desired. The main aim of this step is to identify the assets at risk, the risks associated with these assets and any likely exposure the organisation may face if the threat were to occur. 'Least' and 'worst' possible scenarios are drawn from the group in order to identify the extent of the possible exposure and its importance to the organisation's operations and survival. However, if management wishes to use this exercise as a

means of cost-justification of security measures subsequently to be implemented, then a recognised and tested quantifiable approach is recommended.

The outputs of the three major exercises undertaken by staff in this phase, that is the security review report, the rich pictures and the risk analysis, are combined to form a big picture of the current security situation of the organisation. The big picture is not a deliverable in itself, purely a collation of information from the three sources. This information is then passed on to phase three where the organisation's systems of information and security are analysed in detail. This phase is illustrated in Figure 6.7.

6.4.2.3 Phase 3: Analyse Systems of Information and Security

This stage is the first activity taking place in the conceptual or ideal world (see Figure 6.8 below). It looks at the 'systems' of information in the organisation at a conceptual level, based upon their informational content and how it is used, rather than on physical limitations of current systems, such as computerised accounting modules, or manual information processes. Using the rich pictures, risk analysis findings and the security review as sources of information, root definitions or missions for these ideal systems of information are developed and the associated security issues highlighted.

By looking at the information in a lateral way rather than within current boundaries, it is possible to analyse the information into abstract systems with different factors dictating the boundaries of such systems. This involves considering the type and content of information and how it is used, and then the security issues associated with those systems and the information itself. Root definitions for each of the conceptual systems are then cultivated, using the CATWOE technique. This identifies the system's Customers (beneficiaries or victims), Actors (those who carry out the action), Transformation (action processes), Weltanschauung (meaning for its existence), Owners (systems owners) and Environment (situational constraints). The root definitions and CATWOEs form a framework for a more detailed analysis of these systems is built up in this phase for transferring to the next phase. Risks overlooked in the comparison stage (phase 5) may also be used as inputs to these activities if phase 3 is subsequently revisited.

Human, organisational and strategic factors are considered during the high level analysis of these ideal systems to ensure a balanced and cohesive view is achieved. A more detailed analysis is then carried out, identifying the type of information 'system', its contents, creator, custodian, and users, how and where the information is stored. Security aspects are also studied particularly regarding the sensitivity of the information. The security missions for these core systems are then developed and passed onto the next phase.

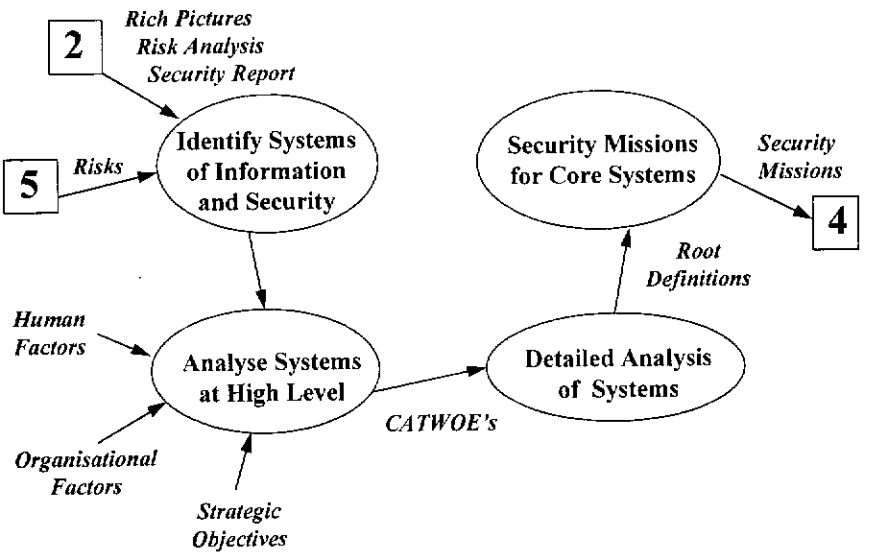

Figure 6.8: Phase 3: Analyse Systems of Information and Security

The application of this phase as designed in theory was found to be difficult to apply during the next phase of the research. The necessary alterations to the activities shown in Figure 6.8 to fit the practical environment are discussed in the next chapter.

6.4.2.4 Phase 4: Model Ideal Information and Security Situation

The root definitions or core missions for each of these systems are used in phase 4, the modelling of the ideal security situation. This phase looks at the risks associated with the creation, transportation, storage, use and destruction of each information type.

Again, ensuring human, organisational and strategic issues are considered, the group then interprets how the aims of integrity, privacy, availability and authenticity can be implemented to ensure an ideally secured situation. Specific security requirements are developed from this ideal situation. These ideals are prioritised by participants to give an indication of the importance attached to each requirement. Figure 6.9 illustrates this phase.

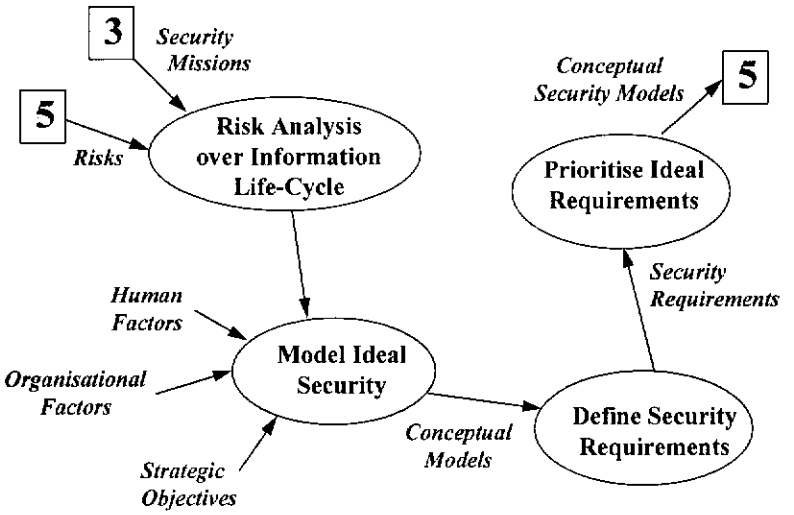

Figure 6.9: Phase 4: Model Ideal Information Security Situation

As with Phase 3, the practical application of these activities was difficult to implement. Changes to this phase are also discussed in the next chapter.

6.4.2.5 Phase 5: Compare Ideal Security with Current Security

The ideal situation developed in phase 4, plus the rich pictures, risk analysis and security report from phase 2, form the input to this phase. A comparison of the ideal models and the situation presently occurring in the real world is undertaken in order to identify any gaps which exist (see Figure 6.10). This comparison should also highlight any problems or risks that have not been addressed in the building of the ideal models, and the group can then return to phases three and four to ensure these omissions are included.

Any changes or desired enhancements arising out of the comparison are then identified. This is virtually a list of needs and wants drawn up from the gap analysis, which must then be collated and integrated to form a set of desired solution requirements. These requirements should define the problem or opportunity being addressed, the specific needs associated and how the solution would integrate into the total picture.

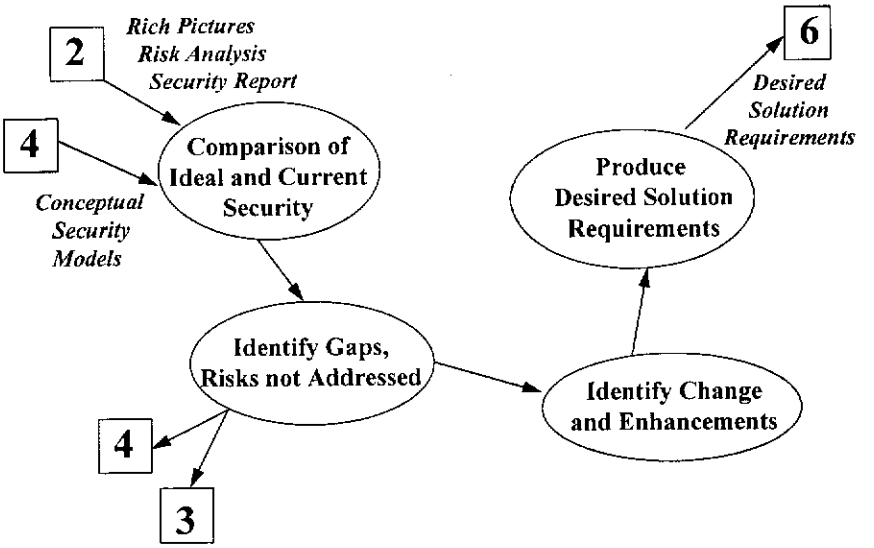

Figure 6.10: Phase 5: Compare Ideal Security with Current Security

6.4.2.6 Phase 6: Identify and Analyse Measures to Fill Gaps

The desired solution requirements developed in the previous phase form the basis for the search and determination of appropriate measures to fill the gaps. As can be seen in Figure 6.11, the first major activity is to scan the wider environment for possible alternative solutions. The sources approached will depend on the solution required, for example, if devices are needed, then vendors or manufacturers would be approached. If procedures need redesigning then possibly an analyst may be consulted. Researchers may be able to provide ideas or guidance for innovative and

unusual requirements. It is important to note at this stage that no alternative be dismissed, but all possibilities be compiled and reviewed.

The review process will allow the most appropriate solutions to be identified, taking into consideration any external constraints (for example, policies, availability and reliability of solutions). These solutions are evaluated and the most desirable and feasible measures chosen. Once these solutions have been decided upon, then the group can prioritise the importance of each with regard to implementation. A prioritised set of recommendations is the output of this phase.

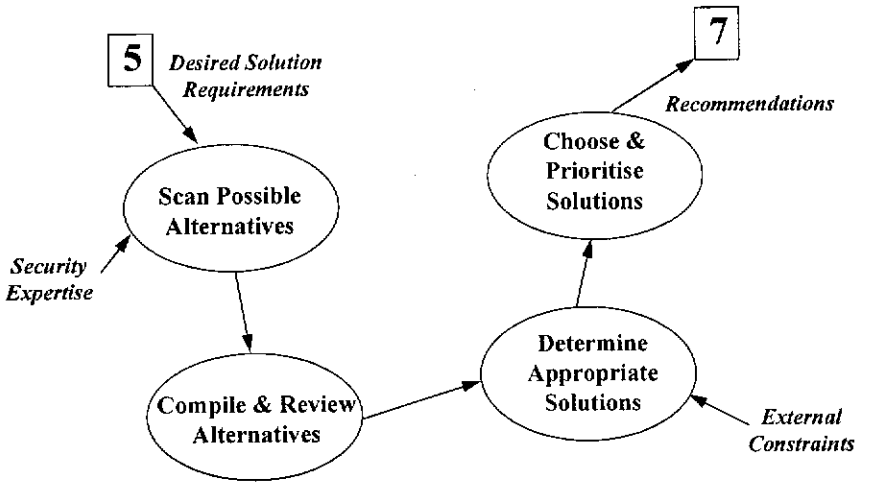

Figure 6.11: Phase 6: Identify and Analyse Measures to Fill Gaps

6.4.2.7 Phase 7: Establish and Implement Security Plan

The recommendations developed in the previous phase are considered by executive management (either a task force, board of directors, or similar) and the preferred solutions are formulated into an action decision. An implementation plan is devised (see Figure 6.12) detailing the tasks involved and the acceptance criteria to subsequently measure the success of the implementation.

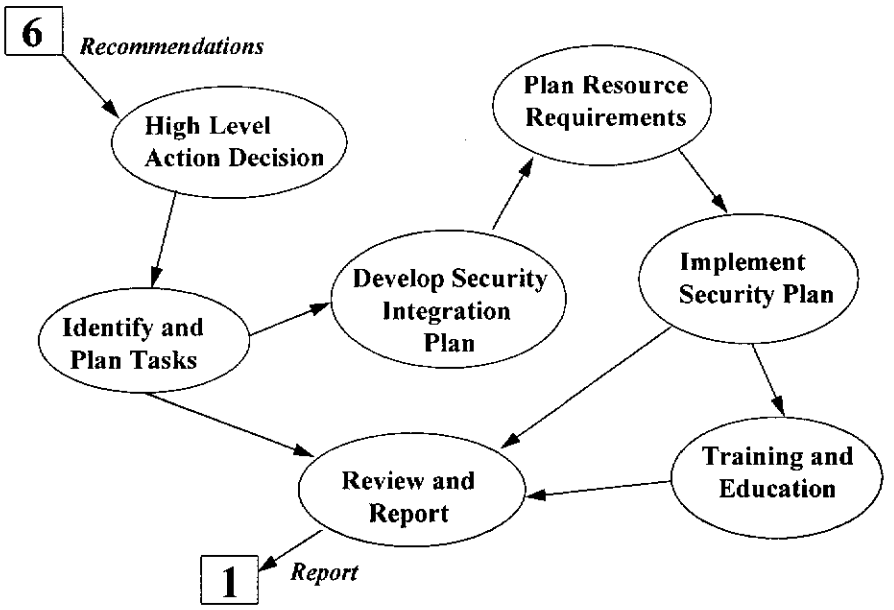

Figure 6.12: Phase 7: Establish and Implement Security Plan

This planning stage also includes consideration of the integration of security into all systems of information, ensuring standards are the same for all systems, but at the same time ensuring the measures are entirely appropriate for each separate system. The dependencies of systems and security measures must also be considered during this phase to ensure the activities of one measure do not interfere with the operations of another.

The resources required to carry out the implementation are then planned and allocated to the tasks. Resources required would include people, skills, time, equipment, costs, training and supervision for each task. The implementation then takes place, and training and education to support the measures implemented is carried out for all staff. On completion of the implementation and training, the exercise is reviewed and success is measured against the criteria established earlier in this phase. The results of this review can form part of input back to the first phase where dynamic factors have necessitated further changes or enhancements, and so the cycle begins again.

6.4.2.8 The Boundary

The boundary around the system illustrates where actions and responsibilities lie in respect to the holons under study. Hence any entity or factor appearing outside the boundary line will be viewed as an external entity over which the system has little control. Those activities appearing within the boundary are the minimum set of activities required to fulfil the root definition previously devised.

The boundary also denotes a demarcation of responsibility for security, however, the problem of securing information after it leaves the confines of this boundary is a difficult prospect with current global networks and open systems facilities.

6.4.3 Naming the Orion Strategy

The Orion Strategy has been named after the Orion constellation of stars. See Appendix F for a discussion of the naming process.

6.4.4 Further Development of the Orion Strategy

A learning process was undertaken as the application of the strategy at the hospital site took place. A number of problems relating to the close alignment of the Orion Strategy with SSM were experienced in the application stage of the research. The model was modified as the security study advanced. The application process and the changes made are discussed in the next chapter.

6.5 CHAPTER CONCLUSION

The Orion Strategy has taken the basic principles of SSM and applied them in theory to information security within an organisation. The involvement of information stakeholders in the planning and management activities is designed to raise awareness of security issues and increase ownership of protective measures. In addition, the Orion Strategy aims to align information security with organisational goals and

missions, and encourages the inclusion of information security as part of the organisational culture and management mind-set. It encourages a holistic approach and a proactive management stance for protection.

Implementing security measures purely for the sake of security can be a waste of scarce and valuable resources. Organisations, therefore, need to analyse their information thoroughly and ensure the appropriateness of security controls before a security program is undertaken. However, if employees within an organisation recognise the need for security measures, the measures are appropriate for the environment and tasks and processes involved, then the security of information will be easier to attain and maintain.

7. APPLICATION OF THE ORION STRATEGY

7.1 CHAPTER INTRODUCTION

In the earlier part of the research it was found that security practices in the health industry were notably poor. This chapter looks into information security management in health care in more detail before discussing the implementation of the Orion Strategy at a private hospital. This section also discusses how the Orion Strategy was modified during its application.

7.2 SECURITY MANAGEMENT IN HEALTH CARE

The importance of security in medical environments has increased world-wide as technology has advanced. For example, the European Commission has been looking into security and safety within the health care industry since the late 1980's and acknowledged the safety issues associated with information systems in health care (Roger-France and Santucci 1991). Security objectives for medical information systems are the same as those for any other information system, namely integrity, availability and confidentiality (Barber and Davey 1996; Blobel and Pharow 1999a; Dietzel 1996; Humphreys 1996; James, Andronis & Paul 1996; Laske 1996; Pangalos and Khair 1996; Shaw 1996; Warren, Furnell & Sanders 1997). The integrity and availability of patient information in hospital and medical records, in particular, is important in the diagnosis and treatment of patients as well as patient privacy (Barber, Vincent & Scholes 1992; Cordonnier and Watson 1998; Laske 1996; Smith and Eloff 1998). The major security vulnerabilities arising for both conventional and electronic health care records are summarised in Table 7.1.

Specific risks, which face organisations in the health care industry, affect not only confidentiality of data held but also the availability of the data and systems as well as the integrity of that data. Medical systems contain highly sensitive information, for example, patient records of fertility and abortions, emotional problems and psychiatric care, sexual behaviours, sexually transmitted diseases, HIV status, substance abuse, physical abuse and genetic dispositions to disease (Rindfleisch

1997). Hospital and other health care systems store data for medical practitioners on treatment practices, the success of surgical techniques and research material.

Security Aim	Details of Risk
Integrity and Availability	Patient records held in separate parts, controlling access to data • defining and agreeing the 'need to know' ie what part of the health record may be disclosed to whom • who controls, and who arbitrates over, such disclosure
Integrity	Quality of records due to varied skill of their authors
Confidentiality	of Subject, health care Practitioner and Third Parties mentioned in records
Authenticity	Attribution of entries in patient records

Table 7.1: ***Security Problems Arising in Health Care Records***
Source: After Gaunt and Roger-France 1996, p11

Reported consequences of insecure information systems in the health care industry include embarrassment or social ostracism of patients following disclosure of sensitive information about mental health, sexually transmitted diseases and adolescent care (Council on Scientific Affairs, 1993) plus drug addiction and genetic fingerprints (Annas 1993). In addition there exists the risk of compromisation of clinical care by inaccurate or missing data resulting from unauthorised modification, system malfunction or errors in program design (Laske 1996; Page, Williams and Boyd 1993); and potential for harm or death if such errors remain unrecognised (Levenson and Turner 1993). Additional risks include financial loss, disruption of activities, failure to meet legal obligations and loss of business (Barber and Davey 1996).

The sources of security risks come from accidental disclosures, unauthorised use of information resulting from insider curiosity and insider subordination (such as spite, revenge or profit), uncontrolled secondary usage by associated organisations, and unauthorised external access (Rindfleisch 1997). Hence security risks emanate from both internal and external sources.

SEISMED (Secure Environment for Information Systems in MEDicine) completed a survey in security awareness as part of the Advanced Informatics in Medicine program established by the European Community. The findings highlighted the low awareness of security issues as well as the low awareness of means for improving security in medical situations (Treacher and Bleumer 1996). In health organisations in the UK in particular, it was noted that even the lowest levels of security measure were not always in place (Barber and Davey 1992 and 1996). In addition to this low security awareness in health care, there is also the problem of the large gap between theory and practice in data security (Louwerse 1996).

Hence the SEISMED team developed a security guidelines package, targeted at four major audiences, the management, IT system end-users, IT and security staff, and general personnel. Data protection instruments in Europe are based upon Article 7 of the COE (Council of Europe) Convention and Article 17 of the EU (European Union) Directive (see Dammann 1996). These require appropriate security measures be taken to protect data from accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination, particularly where data is transmitted across networks. The countries within the European Community are embracing these data protection requirements, and are currently leading the way in security in medical information.

Health care professionals need to understand why it is important to maintain a secure environment for information about patients and patient care. A number of essential components will bring this into being; firstly, a management structure that recognises the responsibility of health care professionals to secure patient data, and secondly, a well structured educational program involving all trainee and professional staff (Gaunt and Roger-France 1996). Information system security in the health care industry is not purely a technical issue, with social and organisational factors also playing a major part (Anderson 1997). Security in health care is a people problem and users remain its greatest threat. Due to the lack of security awareness and deficient procedures, clearly written procedures and codes of conduct are added to this list of essentials (Gaunt and Roger-France 1996; Rindfleisch 1997).

Additional security measures recommended specifically for the health care sector include

- information security policies, procedures and codes of practice (Barber and Davey 1996; Blobel and Pharow 1999a and 1999b; Fowler 1996; Furnell and Sanders 1996; Gaunt and Roger-France 1996; Laske 1996; Rindfleisch 1997; Shaw 1996);
- allocation of security responsibility to a security administrator and all staff (Blobel and Pharow 1999a and 1999b; Corbeel, Corbeel and Hortmann 1996; Furnell and Sanders 1996; Gaunt and Roger-France 1996);
- security education and awareness programs (Blobel and Pharow 1999a; Fowler 1996; Furnell and Sanders 1996; Gaunt and Roger-France 1996; Katsikas 1996; Laske 1996; Rindfleisch 1997);
- risk analysis and contingency planning (Barber and Davey 1996; Blobel and Pharow 1999a; Fowler 1996; Furnell and Sanders 1996; Gaunt and Roger-France 1996; Humphreys 1996; Laske 1996; Warren, Furnell and Sanders 1997);
- logical access controls and system logs (Barber and Davey 1996; Blobel 1997; Corbeel, Corbeel and Hortmann 1996; Dietzel 1996; Fowler 1996; Furnell and Sanders 1996; Holbein et. al. 1997; Laske 1996; Rindfleisch 1997);
- systems development and implementation controls, particularly project management, specification, design, construction, testing, implementation and separate environments (Bakker, van Dorp and van Veenen 1996; Barber and Davey 1996; Gaunt and Roger-France 1996; Rindfleisch 1997);
- quality assurance controls (Gaunt and Roger-France 1996);
- transmission and network controls (Barber and Davey 1996; Blobel and Pharow 1999a; Dietzel 1996; Gaunt and Roger-France 1996; Laske 1996; Rindfleisch 1997); particularly in open systems (Blobel 1997; Bleumer 1996; Klein 1996; Patel and Kantzavelou 1996; Vassilacopoulos, Chrissikopoulos and Peppes 1996);
- physical and environmental security (Dietzel 1996; Fowler 1996; Furnell and Sanders 1996);
- classification of information (Rindfleisch 1997)
- IT facilities management and database security (Furnell and Sanders 1996; Pangalos and Khair 1996); and

- system maintenance and dependability (Dietzel 1996; Furnell and Sanders 1996; Shaw 1996).

The above security measures do not apply solely to health care organisations. These are standard best practice measures, however the list above is seen to be of particular importance in health care environments.

Due to the poor awareness of management and staff in health care organisations there appears to be a need for the building of a 'security culture' within the organisation itself. In Chapter 5 the requirement for security awareness, acceptance of responsibility and action was discussed (see Figure 5.1). For effective security management in health care staff must be *aware* of the need and reasons for security; they must *accept* that to maintain security they will be both constrained and held responsible for their actions when using these systems; and that *action* must be taken to increase awareness and acceptance and thus implement measures to improve security where necessary (Fowler 1996).

7.3 APPLICATION DESIGN AND OVERVIEW

In order to learn how the Orion Strategy could be most beneficially used in a health care environment a pilot application was undertaken at a large private hospital in Perth, Western Australia. As the implementation of the approach took place, the original theoretical model was streamlined and enhanced.

At the time this research was undertaken the hospital was the largest private hospital in Perth with more than 300 beds. Until early 1994 it was a federally-run veterans repatriation hospital with a vigorous role in teaching and research. Upon its sale to the private sector, the hospital extended its care to public and private patients as well as veterans. It remains a teaching and research institution with strong links to the state's major public hospitals and the University of Western Australia. Its funding - and therefore its information exchange responsibilities - encompass the federal Department of Veterans' Affairs, the state and federal Departments of Health, and the private health insurers.

Activities involved in the application included information security education sessions, numerous workshops (involving more than sixty middle and senior managers) and interviews. Data was gathered from these activities in addition to numerous questionnaires at different stages of the testing. The possibility of influence of the researcher on the situation was recognised (see Galliers 1991) and an independent facilitator was used for the workshops. This tactic was employed because it not only allowed independent observation to take place, but also the researcher (who played the role of the 'security expert' in other phases) was less able to directly influence the direction or decisions made within the workshops. Triangulation of data collection methods was used to increase the validity and reliability of the findings.

7.3.1 Application of Phase 1: Acknowledgement of Possible Security Vulnerability

Much of the action involved in this phase of the approach had already taken place prior to the commencement of the research at the hospital. The hospital's mainframe computer system had been recently replaced by a distributed network architecture enabling greater access to information and systems by staff. Management recognised the need for a review of security and had appointed the IS Manager to look into ways of involving senior and middle management in the security planning process. One source of this recognition was the occurrence of a number of security problems, which although minor in impact, were of an embarrassing and nuisance nature. Confidential staff information had been accessed and distributed by unauthorised personnel, confidential patient information was lost or mislaid and hardware had been stolen. It also appeared there was no record of any security review or planning for security in the past for the hospital.

Hospital management was concerned about the confidentiality and integrity of patient and practitioner information and were cognisant of the need for ongoing reliable computer operations. The security of competitive hospital information had also become a concern of hospital executives in the planning of strategic direction and

activities. The completion of this stage was totally in line with the theoretical model for phase 1. Figure 7 illustrates the activities carried out in this phase.

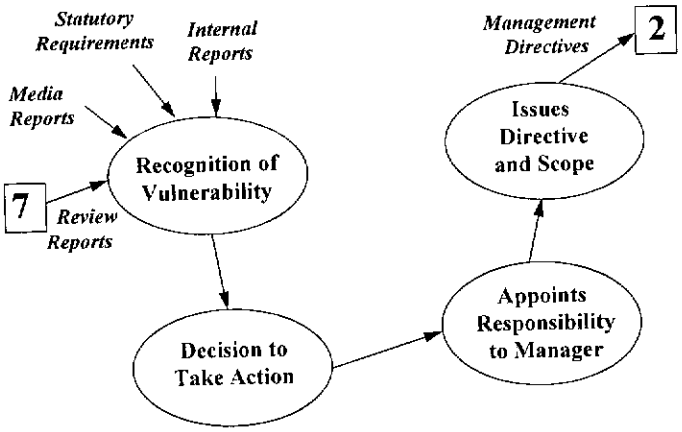

Figure 7.1: ***Actual Activities carried out in Phase 1***

7.3.2 Application of Phase 2: Analyse Current Security Situation

An initial written memo was sent to all senior and middle management staff to advise executive management's decision to look more closely at information security within the hospital. A seminar was held to inform staff of the proposed course of action. At the same seminar the researcher presented a security awareness session explaining the aims and scope of information security, the types of abuse associated with computerised information, the level of abuse in Australia and overseas, the current status of information security management, and the management needs arising.

The researcher also carried out a security review, by physical inspection of the computing and networking facilities, observation of the working environment, the flow of information and paper throughout the hospital, and study of written procedures, manuals and other working documents. Staff were not aware that this review was taking place, as it preceded the security education session. It should be noted that this review was not an audit of the informational content of any computing system, but purely a review of security procedures and controls within the working and computing environment.

The first participative workshop was held with senior and middle managers, or where managers were unable to attend another staff member attended as their delegate. The majority of areas of the hospital were represented at each of these workshops. The aim of the first workshop was to analyse the current security situation and identify problem and potential problem areas within the hospital situation.

As the number of managers involved totalled approximately sixty, it was necessary to hold three workshops covering the same topics with twenty attendees at each. This necessitated the collection of workshop findings over the three groups.

In the theoretical approach the output of this stage was a rich picture of the current situation. However, the participating managers showed little interest in drawing rich pictures, and preferred listing problem situations in narrative form on the whiteboard.

A rich picture was subsequently developed by the IS Manager, the workshop facilitator and the researcher at the conclusion of the first round of workshops (see Figure 7.2).

The workshops also identified potential security risks associated with problem and potential problem areas. The risks were considered under the headings of 'lack of confidentiality', 'lack of integrity' and 'lack of availability'. Table 7.2 summarises the high level risks identified in these workshops.

Phase 2 was carried out in line with the theoretical model. See Figure 7.3 for the activities carried out during this phase of the research.

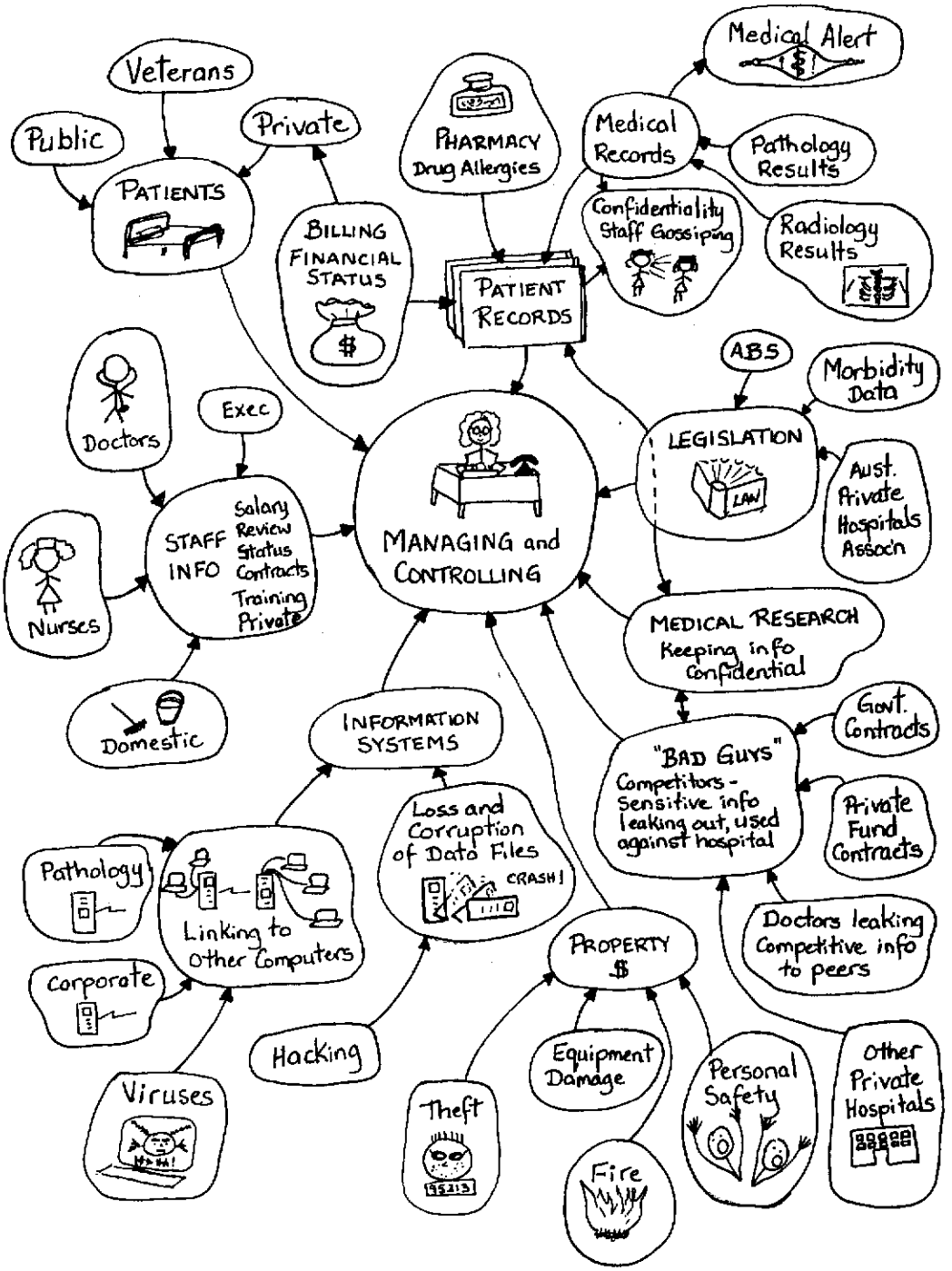

Figure 7.2: Rich Picture of the Problem Situation at the Hospital

Risk Characteristic	Type of Information	Security Risk
Lack of Confidentiality	Patient Information	- patient embarrassment - litigation
	Staff Information	- staff embarrassment, possible ostracism - staff unrest - staff lack of confidence in employer - motivation for abuse
	Hospital Information	- competitors taking market share - competitors taking new ideas - competitors taking research - loss of reputation - non-compliance with legal and statutory requirements
Lack of Integrity	Patient Information	- patient death - patient misdiagnosis or mistreatment - litigation
	Staff Information	- staff mistreatment or disadvantage - litigation
	Hospital Information	- non-compliance with legal and statutory requirements - hospital income decline - questionable hospital viability - inaccurate planning and management decisions
Lack of Availability	Patient Information	- patient death - patient mistreatment - duplication of tests and medical procedures - additional reconstruction expense
	Staff Information	- inaccurate staff planning and management decisions
	Hospital Information	- inaccurate planning and management decisions

Table 7.2 Potential Information Security Risks

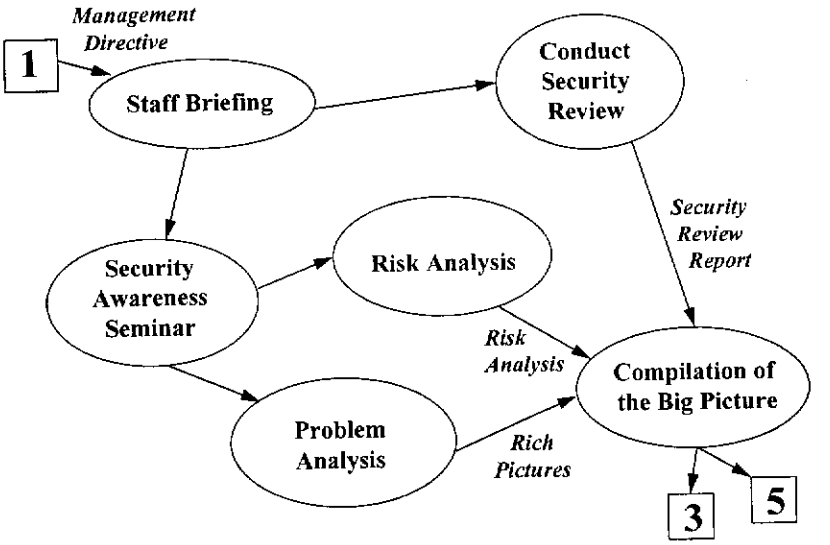

Figure 7.3: ***Actual Activities carried out in Phase 2***

7.3.3 Application of Phase 3: Analyse Systems of Information and Security

Phase 3 in the theoretical model involved the identification and analysis of systems of information and security and a definition of missions for each system. The deliverables of this stage, the mission statements, were to be developed by the use of CATWOE analysis and the defining of root definitions in SSM terms. CATWOE analysis was found to be inappropriate for analysing the security component of the hospital's information. The 'systems of information' were, in fact, not systems, but types of information that supported other systems within the hospital. Each type of information had different security characteristics relating to sensitivity and risks and these characteristics were difficult to include and illustrate via CATWOE's and root definitions.

The hospital's mission is "to provide high quality health care as a unique private teaching hospital". The types of information identified were not based upon computerised information systems, but on functional areas within the organisation designed to fulfil this mission. This link was not particularly strong as the mission statement was a much higher level concept than the information analysis being undertaken. Although the mission did provide a point of reference from which to work, it was not a significant input to this stage. Human and organisational factors

were also not as prevalent in discussion as expected. These were more highly focussed upon in phase 4 during the building of the ideal situation. During the practical application of this phase, therefore, it was necessary to adjust the model to enable types of information and their security characteristics to be identified. Hence, a second set of workshops was held to analyse the information used in the hospital and to draw up a security profile of this information. This involved identifying and classifying information used by type, identifying the source or author of the information, determining the sensitivity of each information type and possible risks or threats to that information.

Table 7.3 illustrates the information classification worksheet used in the analysis. In order to collect this information the participants were required to complete a questionnaire presented in the same format as Table 7.3 with an additional page of explanation and instructions. Results of the questionnaires were collated and presented at the following workshop.

A final rating of the sensitivity of each type of information was assigned after collation of the questionnaires and discussion at the workshops. Following additional discussion of risks and exposures participants were requested to prioritise areas for attention, again via a questionnaire. The prioritisation results were collated and presented back to the group and discussed before final ratings were assigned.

Information Classes	Categories within Information Class	Author /Custodian	Sensitivity
Patient	Medical Record	Doctors, Nurses, Administration & Admissions Staff.	3
	Pathology	Pathologists.	3
	X-Ray	Radiologists.	3
	Pharmacy	Pharmacists.	3
	Billing	Administration.	3
Staff	Personnel Information	Personnel Manager.	3
	Payroll	Personnel Manager.	4
	Clinician Profiles	Medical Services.	3
	Security Incidents	Security Manager.	3
Hospital Management	Executive Hospital Statistics	Executive.	3
	General Hospital Statistics	Medical Services & Clinical Services.	2
	Executive Minutes	Executive.	3
	Committee Minutes (HCP, AHP/SD, Nursing Policy)	Clinical Services.	2
	Policies	Department Heads.	2
	Financial Reports	Finance Department & Department Heads.	3
	Departmental Budgets	Department Heads.	3
	Pharmacy Financials	Pharmacy.	4
	Contracts	Medical Services.	3
	Hospital Keys Information	Fire & Security.	3
	Security & Fire Reports	Fire & Security.	3
	Restricted Security & Fire Procedures	Fire & Security.	4
Hospital Operations	All Procedures	Department Heads.	2
	All Manuals	Department Heads.	2
	Policy & Procedure Manuals	Clinical Services.	2
	Operating Statistics	Clinical Services.	3
	Doctors' Reference Cards	Clinical Services.	3
	Statistics & Reports	Library.	2

Sensitivity Legend
1 = Public - no restrictions
2 = Hospital Staff Only
3 = Defined Group of Staff
ie Dept or Section
4 = Restricted to Stated Individuals

Table 7.3: Information Classification Worksheet

Figure 7.4 details the activities carried out during this phase of the application.

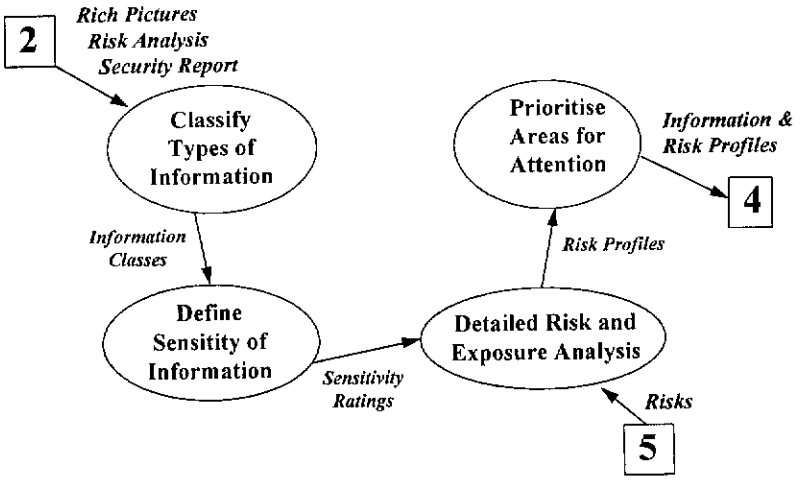

Figure 7.4: ***Actual Activities carried out in Phase 3***

7.3.4 Application of Phase 4: Model Ideal IS Security Situation

Using the information and risk profiles from the previous phase an analysis was undertaken to determine the risks of each information type over its life-cycle. The life-cycle phases considered were information creation, transportation, storage, use and destruction. The principles of integrity, confidentiality and availability were applied and an ideal scenario developed.

It was originally intended to use conceptual modelling as per SSM, however, this type of modelling was not able to fully illustrate the ideal security situation. This was possibly due to the security situation under study being contextual rather than systemic, its influence extending across the boundaries of the organisation's activity systems. Security was viewed, not as a system in itself, but a supporting mechanism for these other systems.

In the workshops for modelling the ideal situation, consideration was given to many human factors. These factors included the user friendliness of controlled situations,

potential changes in staff work patterns, the implication of controls on staff self-worth and self-confidence, the implication of controls on staff loyalty, the influence on freedom in decision making and the desire for preventative security management in preference to a defensive policing function.

Organisational factors influencing the design of the ideal security situation included organisational policies, organisational structure, management reporting procedures and lines of responsibility, physical layout of the hospital and administration buildings, and current work practices. Other factors which affected planning indirectly were legal and statutory requirements posed by state and government bodies, and other hospital governing organisations.

The hospital had a clearly defined vision, mission and set of strategic objectives (see Appendix F for full details). The hospital's goals are:

1. To be recognised by doctors, patients, families and the local community for giving better care and service than any other private hospital.

2. To create a working environment where people achieve and feel valued.

3. To create a unique private teaching hospital environment that results in local, national and international recognition for excellence.

These goals formed a firm basis in the development of the ideal security situation. It was necessary for the new scenario to assist in achieving these goals rather than acting as an obstruction. Participants discovered that security was an integral part of other systems designed to specifically address these goals, and that security principles were of vital importance in achieving these goals. The second goal was of particular assistance in human considerations and the effect on staff and patients of desired security levels.

Information Classes	Information Categories within Classes	Confidentiality	Integrity	Availability
Patient	Medical Record Pathology X-Ray Pharmacy	• limit access to authorised personnel only • protect highly sensitive information in storage and transmission • secure destruction of obsolete information	• procedures for addition, modification and deletion of information • integrity checking and verification of information in storage • version control • integrity checking and verification of information in transit	• ensure safe storage • efficient access methods for fast retrieval • information formatted to enable easy interpretation of data
Staff	Personnel Info Payroll Clinician Profiles Security Incidents	• limit access to authorised personnel only at given levels • protect highly sensitive information in storage and transmission • secure destruction of obsolete information	• procedures for addition, modification and deletion of information • integrity checking and verification of information in storage • integrity checking and verification of information in transit • logging of output distribution	• ensure safe storage • backup info and store safely on-site and off-site • information formatted to enable easy access to and interpretation of data
Hospital Management	Hospital Statistics Exec Minutes Committee Minutes Policies Financial Reports Depart'l Budgets Pharmacy Finance Contracts Hospital Keys Security & Fire	• limit access to authorised personnel only at given levels • protect highly sensitive information in storage and transmission • secure output containing sensitive information • secure destruction of obsolete information	• procedures for addition, modification and deletion of information • integrity checking and verification of information in storage • integrity checking and verification of information in transit • logging of output distribution • version control	• ensure safe storage • backup computerised info and store safely on-site and off-site
Hospital Operations	Oper Procedures Oper Manuals Policy & Proc Manuals Operating Stats Doctors' Ref Cards Stats & Reports	• limit access to authorised personnel only • protect information in storage and transmission • secure destruction of obsolete information	• procedures for addition, modification and deletion of information • integrity checking and verification of information in storage • version control	• ensure safe storage • backup computerised info and store safely on-site and off-site

Table 7.4: Defining Security Requirements

The ideal situation was brainstormed on the whiteboard in the workshops with ideas, modifications and enhancements added to the picture as discussion progressed. Once the ideal scenario was developed and agreed upon, the managers set to defining the specific security principles required to produce that ideal. These principles were defined in general terms rather than specific security products or procedures (see Table 7.4). These requirements were again developed in a workshop setting with the same group of participants. The final activity of this phase was the ranking of these requirements by the participating managers. The highest ranking requirements almost unanimously related to the confidentiality of patient records and competitive hospital information.

With the exception of the use of SSM conceptual models, this phase was executed in line with the theoretical model (see Figure 7.5).

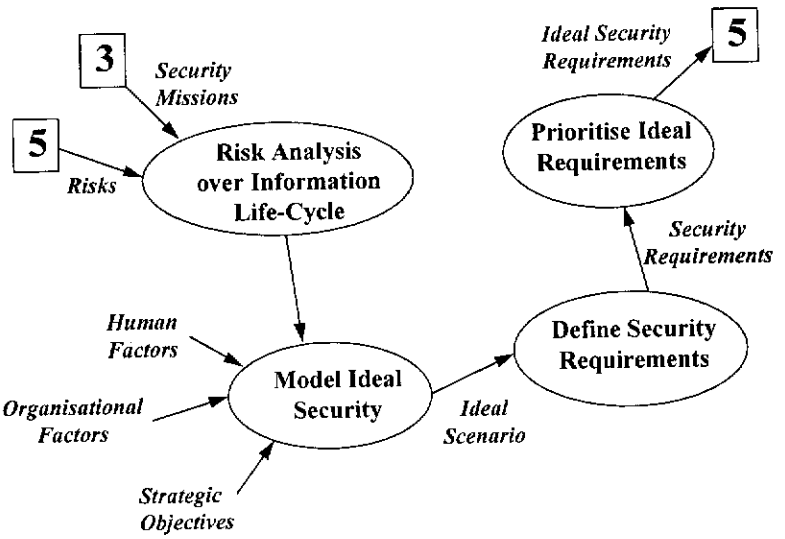

Figure 7.5: ***Actual Activities carried out in Phase 4***

7.3.5 Application of Phase 5: Compare Ideal with Current Security

The first activity undertaken in phase 5 was to compare the current security situation with the ideal security defined in phase 4. The security review highlighted current areas of concern where control measures were insufficient, and the risk analysis and rich picture added areas of vulnerability. Although the ideal security requirements from the previous phase were not in the same format as the documents portraying the current situation, gaps and differences were easily identifiable.

The workshop participants identified any changes (removals, modifications or additions) that were necessary for the current environment to match the ideal, under each information type heading. During this exercise there was much revisitation of phases 3 and 4 as additional risks were identified during the discussion.

Taking the current measures which were in place and effective, and those changes and enhancements still necessary, desired solution requirements were drawn up (see Tables 7.5(a) - 7.5(d)). These tables also summarised the adequacies and shortcomings (gaps) in the current situation.

Information Classification	Sensit -ivity	Desired Solution Requirements	Gaps in Current System
Patient Information Medical Record Pathology X-Ray Pharmacy	 3 3 3 3	**Information Management** - responsibility for security of patient info assigned to manager - organisational policies for the security of patient information - classification of patient information to determine sensitivity - full risk analysis of patient information giving risk profiles - procedures for handling sensitive patient information - education of staff in handling sensitive patient information	**Information Management** - no assignment of responsibility for patient information security - no organisational security policies relating to patient information - no classification of patient information - partial risk analysis of patient information only - no procedures for handling sensitive patient information - no education of staff in handling sensitive patient information
		Logical Access Security - assign different levels of user access authorisation - restrict ability to read, write, delete to authorised users - logging of actions performed on computerised functions	**Logical Access Security** - insufficient differentiation of users - not fully computerised - insufficient access control facilities in user authorisation tables - limited logging undertaken
		Physical Access Security - secure data storage areas - restrict physical access to patient records - restrict physical access to servers, workstations and fax machines - secure the movement of hard copy material - secure destroyal of sensitive documents relating to patients	**Physical Access Security** - specified storage areas not secured - workstations and fax machines easily viewed by visitors - hard copy records left unattended - easy access to files in trolleys - sensitive documents not destroyed
		Backup and Recovery - written backup procedures - logs of backups - secure storage of backups onsite and offsite - test backups before storage	**Backup Recovery** No gaps found

Table 7.5(a): Desired Solution Requirements Worksheet – Patient Information

Information Classification	Sensit -ivity	Desired Solution Requirements	Gaps in Current System
Staff Information Personnel Payroll Clinician Profiles Security Incidents	 3 4 3 3	**Information Management** - responsibility for security of staff info assigned to manager - organisational policies for the security of staff information - classification of staff information and security incidents to determine sensitivity - responsibility for confidentiality of security incident information - full risk analysis indicating risk profiles for staff information - procedures for handling sensitive staff information - education of staff in handling sensitive staff information	**Information Management** - no assignment of responsibility for security of staff information - no organisational security policies relating to staff information - no classification of sensitivity of staff information - responsibility for confidentiality of security incidents assigned to Security Manager - partial risk analysis undertaken - no procedures for handling sensitive staff information - no education of staff in handling sensitive staff information
		Logical Access Security - assign different levels of user access authorisation - restrict ability to read, write, delete to authorised users - logging of actions performed on computerised functions	**Logical Access Security** - insufficient differentiation of users in payroll and personnel systems - insufficient access control facilities in user authorisation tables within payroll and personnel systems - limited computerised logging
		Physical Access Security - secure data storage areas - restrict physical access to staff records - restrict physical access to servers, workstations and printers - secure destroyal of sensitive documents relating to staff	**Physical Access Security** - specified storage areas not secured - workstations and printers not fully secured - easy access to files in filing cabinets - sensitive staff documents not destroyed
		Backup and Recovery - written backup procedures - logs of backups - secure storage of backups onsite and offsite - test backups before storage	**Backup Recovery** No gaps found

Table 7.5(b): Desired Solution Requirements Worksheet – Staff Information

Information Classification	Sensit -ivity	Desired Solution Requirements	Gaps in Current System
Hospital Management Information Hospital Statistics Executive Minutes Committee Minutes Policies Financial Reports Depart'l Budgets Pharmacy Finance Contracts Hospital Keys Security & Fire	 3 3 2 2 3 3 4 3 3 4	**Information Management** - responsibility for security of hospital management info assigned to manager - organisational policies for the security of hospital management information - classification of hospital management information to determine sensitivity - full risk analysis indicating risk profiles for hospital management information - procedures for handling sensitive hospital management info - education of staff in handling sensitive hospital management information	**Information Management** - no assignment of responsibility for security of hospital management information - no organisational security policies relating to hospital management information - no classification of sensitivity of hospital management information - partial risk analysis undertaken - no procedures for handling sensitive hospital management information - no education of staff in handling sensitive hospital management information
		Logical Access Security - assign different levels of user access authorisation - restrict ability to read, write, delete to authorised users - logging of actions performed on computerised functions	**Logical Access Security** - insufficient differentiation of users hospital management systems - insufficient access control facilities in user authorisation tables within hospital management systems - limited computerised logging
		Physical Access Security - secure data storage areas - restrict physical access to hospital management records - restrict physical access to servers, workstations and printers - secure destroyal of sensitive documents relating to hospital management	**Physical Access Security** - specified storage areas not secured - workstations and printers not fully secured - easy access to files in filing cabinets - sensitive hospital management documents not destroyed
		Backup and Recovery - written backup procedures - logs of backups - secure storage of backups onsite and offsite - test backups before storage	**Backup Recovery** No gaps found

Table 7.5(c): Desired Solution Requirements Worksheet – Hospital Management Information

Information Classification	Sensit -ivity	Desired Solution Requirements	Gaps in Current System
Hospital Operations Information Operating Procedures Operating Manuals Policy & Procedure Manuals Operating Statistics Doctors Reference Cards Stats & Reports	 2 2 2 3 3 2	**Information Management** - responsibility for security of hospital operations info assigned to manager - organisational policies for the security of hospital operations information - classification of hospital operations information to determine sensitivity - full risk analysis indicating risk profiles for hospital operations information - procedures for handling sensitive hospital operations info - education of staff in handling sensitive hospital operations information	**Information Management** - no assignment of responsibility for security of hospital operations information - no organisational security policies relating to hospital operations information - no classification of sensitivity of hospital operations information - partial risk analysis undertaken - no procedures for handling sensitive hospital operations information - no education of staff in handling sensitive hospital operations information
		Logical Access Security - assign different levels of user access authorisation - restrict ability to read, write, delete to authorised users - logging of actions performed on computerised functions	**Logical Access Security** - insufficient differentiation of users hospital operations systems - insufficient access control facilities in user authorisation tables within hospital operations systems - limited computerised logging
		Physical Access Security - secure data storage areas - restrict physical access to hospital operations information - restrict physical access to servers, workstations and printers - secure destroyal of sensitive documents relating to hospital operations	**Physical Access Security** - specified storage areas not secured - workstations and printers not fully secured - easy access to files in filing cabinets - sensitive hospital operations documents not destroyed
		Backup and Recovery - written backup procedures - logs of backups - secure storage of backups onsite and offsite - test backups before storage	**Backup Recovery** No gaps found
Transmission of Computerised Information	All Levels	- encryption of sensitive data within the intranet - filtering and restriction of data to and from the Internet - secure Intranet from Internet access	- no encryption on sensitive data transmission within the Intranet - no firewall (filtering or restriction of data) between Intranet and Internet - no regulation of Internet activities

Table 7.5(d): Desired Solution Requirements Worksheet – Hospital Operations Information and Transmission of Computerised Information

The activities carried out during this phase were identical to the theoretical model (see Figure 7.6).

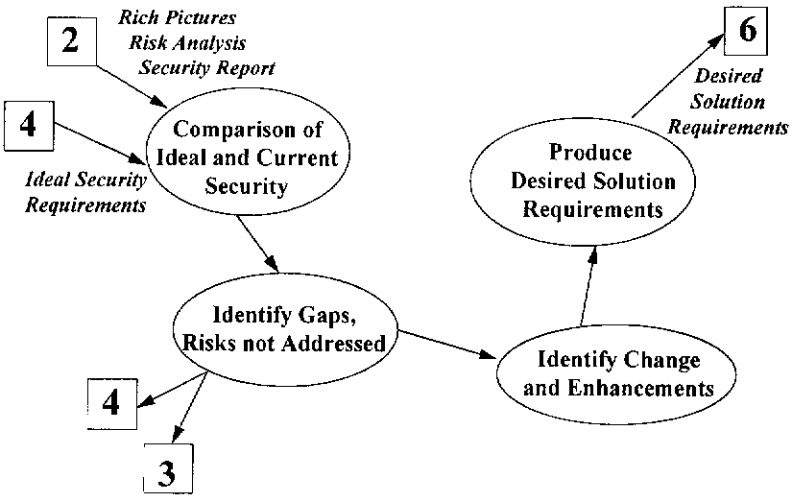

Figure 7.6: ***Actual Activities carried out in Phase 5***

7.3.6 Application of Phase 6: Identify and Analyse Measures to Fill Gaps

Phase 6 of the implementation commenced with an investigation of possible security measures to meet the desired solutions requirements from the previous phase. As the managers had little knowledge of security products and procedures, the researcher provided information and material on possible solutions. Alternative solutions were discussed and action options presented. The majority of solutions required for the hospital were procedure oriented, for example, the development of a corporate security policy and producing guidelines for ongoing classification of information and records management.

Not all recommended solutions were accepted by the participants. Choices were made where it was necessary to determine the most feasible and appropriate solution. For example, to protect corporate computerised information systems from abuse emanating from the Internet, management needed to decide whether to install a

sophisticated set of firewalls (and efficient means of monitoring them), or physically segregate the corporate intranet system from systems with Internet accessibility.

Compromises were necessary in the determination of the most feasible and appropriate solutions. Some of these limitations were posed by financial consideration, excess computer capacity and staff availability to carry out tasks. For example, the production of logs to record all user access activities was desirable in the perfect security situation, however the overheads of such a solution were highly undesirable. Not only does extensive logging slow down user access time but it also uses extensive computer storage space due to the large number of activities involved. In addition, staff would need to review the entries to ensure users had authorisation to perform the related action. It was agreed that logs would be recorded for actions on sensitive information only, rather than all user activities. Facilities to regulate logging which were included in the network management software would also be utilised to assist in this function.

Several sections of the computer network were still being set up and many of the ideal measures were able to be included in these systems as they were being developed and installed. Many of the solutions were the same for different information types. For example, the destruction of confidential information was solved by the installation of shredders across the hospital. Education was another area listed under numerous headings. It was decided that new staff needed to attend an education session as part of the hospital's induction program, and subsequent sessions would be held on a regular basis for all staff.

The final activity to take place in this phase was a prioritisation of the chosen solutions in preparation for the development of an action plan. This was achieved by a questionnaire given to the participants at the completion of the workshops centred on this phase.

This phase of the model was not carried out in a linear sequence as shown on the theoretical model. Although each activity was carried out, the first three activities were, in essence, combined with much movement between activities. Possible

solutions were identified for a particular security area (for example, physical access control) and information on each presented for consideration. These were discussed by the managers, where constraints and other considerations were brought to light. The most appropriate and desirable solutions were then chosen and attention moved to the next security area. Where no solution was found to be acceptable, further scanning of possible measures took place.

The choice of solutions actually took place before the prioritisation for action, which was a separate activity in itself (see Figure 7.7). Table 7.6 contains a summarised version of the recommendations submitted.

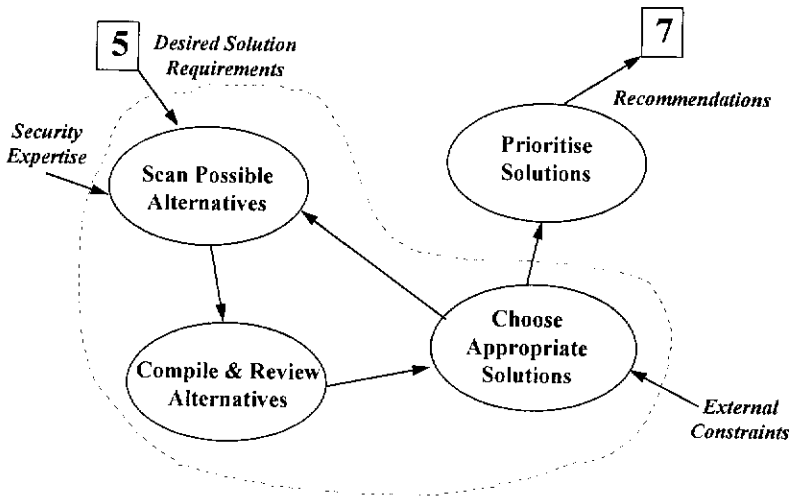

Figure 7.7: ***Actual Activities carried out in Phase 6***

	Recommendation Summary
1	A corporate information security policy be developed, stating the management's goals and stance, indicating its commitment to the integrity, confidentiality and availability of information within the hospital. Guidelines indicating how this policy is implemented within the organisation should be included.
2	A set of guidelines be established for the classification of information within the hospital and a records management system put in place. All confidential information should be labelled with its classification and allowed range of distribution. Develop written procedures for the production and handling of confidential information and ensure staff have copies of these procedures.
3	A full risk analysis be undertaken regarding the physical security of patient, personnel and corporate information, including considerations of disaster recovery planning. This will quantify risks and provide guidelines for financial outlays on security measures to ensure their cost-efficiency.
4	The responsibility for information security be allocated to a trusted employee. This staff member should be a full-time employee, with the knowledge and experience appropriate for the position. This person must be given the authority to carry out actions relating to security issues.
5	A security education program be developed and attended by all staff. This program should be incorporated into the hospital's induction program for new staff.
6	The current confidentiality agreement signed by staff be revised to reinforce the corporate security policy, and in order to be enforceable in a court of law, include the consequences of non-compliance with the terms of agreement.
7	Review in detail the physical security around manual storage areas of confidential information. Access should be restricted to only those staff members who need the information in their areas of work. Equipment housing documents should also be secured.
8	Review the physical security around workstations, fax machines and printers to ensure confidential information is not compromised. Install shredders in all work locations dealing with confidential information relating to patients, staff and hospital planning.
9	Develop a system to restrict access to computerised information and software via authorisation tables, access control matrices and limited user views to databases.
10	Produce system logs for activities on confidential information on computer systems, highlighting activities which may indicate problems. These logs must be checked and followed up where necessary.
11	Install firewalls (gateways and/or intelligent routers) on interconnected computer systems to restrict incoming and outgoing data and messages.
12	Restrict the hospital's connection to the Internet to stand-alone workstations, or totally isolated networked computers. Using firewalls, restrict TCP/IP functions available to those required to achieve job goals, for example, email and ftp. Block or install secure versions of insecure facilities such as Telnet, Remote Logins, Remote Procedure Calls, etc.
13	Retain current computer backup procedures to ensure continued availability of computerised systems, including data and software backups as well as hardware backups. Ensure backups are stored securely both on-site and off-site, and are tested before storing.

Table 7.6: Summarised Version of Recommendations

7.3.7 Application of Phase 7: Establish and Implement Security Plan

Phase 7 of the implementation commenced with submission of the recommendations to the Executive Director of the hospital. After deciding to take immediate action, he then took on the overall responsibility for information security and a small task force was established to activate and manage the design and implementation of the chosen security measures. A two year plan was developed to integrate security measures into normal hospital and administrative operations, and implementation of high priority issues commenced immediately. Resource requirements were identified as part of the action plan, the most prominent factor being the availability of staff to undertake tasks.

At this time the architectural plans for a new hospital building complex were near completion, and the task force moved quickly to alter the designs to incorporate the physical security recommendations. Another high priority was the classification of information and the implementation of a secure records management system. All hospital staff were required to complete a questionnaire detailing the information they used and stored. The analysis of this information for the entire hospital required significant effort, however, the results were highly beneficial. Much duplication was found as clear ownership of information had not previously been defined. It was also found that confidential information was stored in insecure locations and obsolete documentation held unnecessarily. The task force was then able to design an efficient and secure records management system for the hospital.

A security education program was developed and implemented as a priority area, firstly into the hospital's induction program and then into ongoing sessions for all staff. Another priority area was the protection of hard-copy material in transportation and the physical distribution of mail and medical information is now secured in locked, supervised trolleys. Shredders were quickly installed around the hospital, particularly in areas handling confidential information.

The implementation plan developed is still being executed. Affected staff are being trained as each section of the plan comes to fruition. An ongoing reporting function

has been established by the task force, and regular meetings are held to review progress against the plan.

The practical implementation of this phase was close to the theoretical model. However, the activity to establish a task force was not recognised in the theoretical model, and was considered a significant step in the implementation. Accordingly, this activity has been added to the model. The establishment of the action plan, the integration of security tasks and planning resource requirements, three separate activities in the theoretical model, were carried out as one task in the implementation and have been illustrated to that effect in the actual model. The actual tasks carried out are reflected in Figure 7.8.

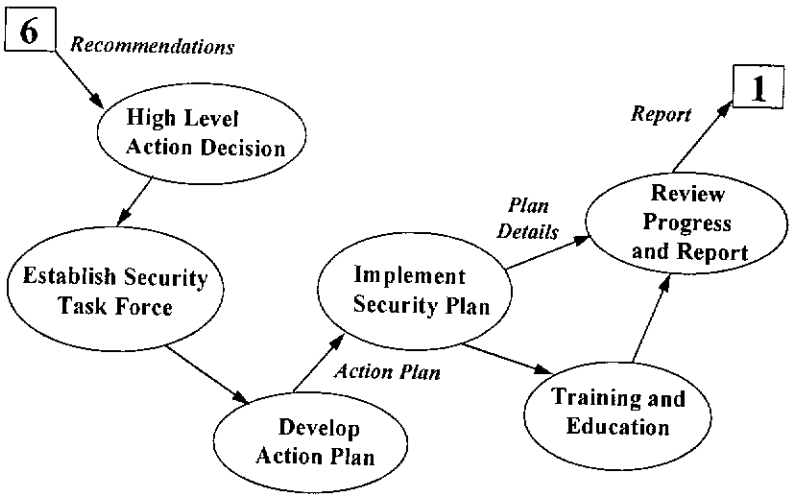

Figure 7.8: ***Actual Activities carried out in Phase 7***

7.3.8 Application of the High Level Orion Model

The seven phases or activities illustrated in the theoretical model were completed in the same sequence during the practical application, however the fit of the process and tools for the overall model was not ideal. Several alterations to the model are recommended based upon its application at the hospital.

Changes to the original high level model are illustrated in Figure 7.9.

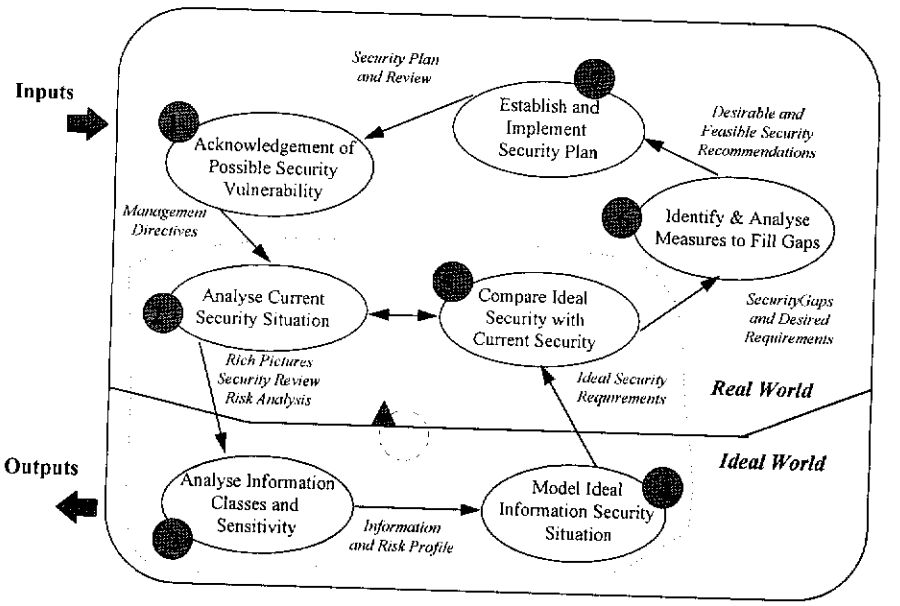

Figure 7.9 The High Level Orion Strategy after Modifications

7.3.8.1 Systems Thinking World

One of the basic underlying problems was the assumption that the research would be systems based. It was, however, predominantly contextual. The move between the 'Real World' and the 'Systems Thinking World' required reconsideration. Phases 3 and 4 which are contained within the 'Systems Thinking World' were not systems based in actuality as the 'systems' considered were not human activity systems as per SSM, but the security needs of information types. A system is a set of elements connected together to form a whole, showing properties of the whole rather than properties of its component parts (Checkland 1981, p3). Information security is not in itself a system as it has no properties as a whole, it is a combination of a number of products and procedures which support other hospital systems. The approach is concerned with the environment of the information, hence it is contextual in nature, rather than systemic. Hence it is recommended that the 'Systems Thinking World' in the Orion Strategy be re-labelled 'Ideal World'.

It follows, therefore, that the tools used in SSM for the analysis of systems, i.e. root definitions and conceptual models, need to be adapted for 'non-systems' analysis. As SSM requires adapting to the given situation, the flexibility of the methodology allows these modifications to be encompassed in the application of the theoretical model. The activity carried out in phase 3 has thus been re-labelled from "*Analyse Systems of Information and Security*" to "*Analyse Information Classes and Sensitivity*" and the final flow to phase 4 changed from "*Security Missions (CATWOEs and Root Definitions)"* to "*Information and Risk Profiles*". Similarly, phase 4 was also re-labelled from "*Model Ideal IS Security Situation*" to "*Model Ideal Information Security Situation*" and the flow to phase 5 from "*Conceptual Security Models*" to "*Ideal Security Requirements*".

7.3.8.2 Links Between Phases 2, 3, 4 and 5

Phases 2, 3, 4 and 5 tended to be carried out as one large activity. The revisiting of prior activities is encouraged in SSM and this was also so in the Orion Strategy. Discussion in the workshops flowed from the current situation for a particular information type to the ideal, and then compared before moving on to the next information type. The activities were logically separate, however in practice the separation was not clearly visible. Participants appeared to prefer discussing one information type at a time, possibly because the security requirements were quite different for each. For example, information types which were highly computerised required different physical, logical and networking security measures to those information types that were predominantly manual. Similarly, security considerations for the hospital's financial information were entirely different to patient record information. The logical combining of the four phases is illustrated by the broken line in Figure 7.9, encapsulating the four phases which formed an internal cycle.

7.3.8.3 Link Between Phases 7 and 1

The cyclical nature of the strategy is designed to create feedback so the organisation is in a position to see new or changed vulnerabilities, i.e. back to phase 1.

Unfortunately, the review procedures had not been completed when the research finished. However, a number of activities had been commenced to establish the review stage in order to feed information back to management.

7.4 CHAPTER CONCLUSION

The Orion Strategy has been developed as an alternate approach for planning and managing information security within business organisations. This approach incorporates high user involvement in an endeavour to improve the planning and management of information security.

Practical application of each phase of the Orion Strategy within the hospital is discussed. The main areas of learning which emanated from this practical stage of the research include:

- Information security is contextual and not systemic
- Difficulty in defining "systems" of information and security, and this activity was replaced by a classification of information
- Non-fit of CATWOEs and Root Definitions as tools for defining the essence of the systems under study. These were replaced by profiles of the information and risks and ideal security requirements.
- Reluctance of participants to draw rich pictures
- The cyclical nature of Phases 2, 3, 4 and 5 for each information type.

There was a high involvement of staff in the workshops over the entire application of the model and the project also received a high level of commitment from the hospital's senior executives.

8. FINDINGS AND LIMITATIONS

8.1 CHAPTER INTRODUCTION

This chapter discusses the findings from the application of the Orion Strategy at a private hospital and then limitations associated with the research. The findings relate to both the *content* of the research, i.e. what was the level of security management before and after the research; and the *process*, i.e. what was learned from application of the model?

Findings relating to the content of information security management are covered initially by examining ratings of the implementation of recommended security measures within the hospital at different stages during the research. These ratings indicate how security management practices changed at the hospital over the period of the research.

The process of using the Orion Strategy is also reviewed with reflections upon the way the research took form and the underlying methodology. This section discusses the use of SSM as a basis for the Orion Strategy and presents an alternative model emerging from subsequent reflection following completion of the practical application at the hospital.

8.2 FINDINGS

The theme of the research centres upon the improvement of information security management, encouraging a greater level of ownership of security measures by information stakeholders. As discussed in the previous chapter the application of the Orion Strategy encompassed a high level of user involvement and resulted in a security plan devised and implemented by the staff of the hospital. This application activity was not intended to test the model as such, because the model was developed as the research progressed. The main activity in this latter part of the research has been focussed on honing the high level Orion model and building the lower levels as the study progressed. This is characteristic of action research projects.

The first finding relates to the application of the Orion Strategy resulting in an improvement in information security management at the hospital. The same security measures used in the study in Chapter 4 have been applied to the hospital in order to indicate any change in information security management practices (see Appendix C for an explanation of the security measures included).

8.2.1 FINDINGS RELATING TO CONTENT

8.2.1.1 Findings Relating to Research Theme

Ratings of the implementation of security measures at the chosen hospital were conducted at three stages during the research process. The first stage was prior to the commencement of the research in 1995, then in 1996 mid-way through the application of the Orion Strategy, and finally in 1997, several months after the completion of the research. The ratings over the three time periods are summarised in Table 8.1. As in the earlier study of the Australian organisations, a rating of 1 indicates the measure does not exist and 5 indicates it is fully implemented and active.

Table 8.1 shows that the implementation of security measures has improved over this time frame, with the hospital moving to a rating of 5 in many areas by 1997. Areas receiving early attention can be seen in the improvement between the 1995 and 1996 periods, including the notable rise in procedures relating to systems development.

This increase was due to the hospital reviewing current procedures and developing more secure procedures in order to achieve quality assurance certification. In addition to reformulating controls in the systems development and maintenance area, shredders were installed across the hospital, backup procedures were reviewed and improved, logical access controls were re-evaluated based upon need and the management and supervision of security improved. The architectural plans for the proposed new hospital complex were also redesigned to incorporate higher levels of physical security.

Security Measure	1995	1996	1997
Corporate Policy	1	2	5
Security Planning	1	3	5
Risk Analysis	1	3	5
Contingency Planning	1	3	4
Security Manager	2	4	5
Supervision of Security	1	4	5
Security Education	1	2	4
Quality Assurance	1	5	5
User Responsibility	1	3	5
Physical Access Controls	2	3	4
Logical Access Controls	2	4	5
System Logs & Error Handling	2	3	4
Change Control	1	4	5
Communications Controls	1	2	4
Independent Audits	2	4	5
Backup Procedures	2	4	5
Project Management	2	5	5
User in Development Team	1	5	5
Development Methodology	1	5	5
Requirements Specifications	2	5	5
Systems Documentation	2	5	5
Design Controls	2	5	5
Walk-thrus	2	5	5
Testing Procedures	2	5	5
Separate Environments	1	5	5

Table 8.1 Ratings of Security Measures at the Hospital

All of the measures at the corporate and operational levels showed improvement in the 1997 ratings. Security policy and planning were notably improved with a security manual developed for all staff, this manual including the policy and written procedures. At the operational level firewalls were installed on internet and network connections, procedures for the use of the internet established, and monitoring of internet usage commenced. Other controls relating to the transportation of sensitive

patient information, e.g. pathology results, required hand delivery directly to the ward. Computer screens, printers and fax machines have been repositioned to ensure information could not be seen by the public. Contracts have also been altered so that cleaning staff are only allowed in the buildings during normal working hours and their access to highly sensitive areas is supervised.

The original security task force assigned at the end of the workshops completed the implementation of new and reviewed security measures and the ongoing responsibility for the management of security has been accepted by a six-member security committee, comprising senior staff from the Nursing, Medical Records, Marketing, Library, Information Services and Quality sections. This committee reports directly to the Executive Director of Corporate Services.

It is clear from Table 8.1 that the implementation and active supervision of security measures has increased in the hospital over this three year period, thus positively supporting the premise that information security management has improved following the use of the Orion Strategy.

8.2.1.2 Content of the Workshops

The workshops forming part of this research covered risk analysis, information analysis, security ideals and potential solution analysis. During the initial education session and first set of workshops an overview of the Orion Strategy was given to explain the process to be undertaken. At the commencement of each workshop brief objectives for the session were presented by the facilitator.

Questionnaires relating to workshop contents were distributed after the second set of workshops and then at the completion of the workshops. The final questionnaire contained questions relating to the process undertaken, and sought improvements that could have helped the study. The majority of respondents did not suggest any improvements, and appeared to be quite happy with the content of the workshops as suggested by these comments:

"Enlightening, relevant issues raised. Certainly heighten concerns that were already held".

"Content was tabled well for easy understanding".

"Content was excellent and covered all issues".

However, it appears that some managers would have liked more information or clarification of the objectives as indicated by these comments:

"Presentation fairly clear, although the aim of the various sessions wasn't made very clear at the start. Articulate the aim, purpose at the commencement of each session".

"Sometimes I don't think people were aware of the purpose of particular segments and why they were there - this could have been made clearer in the introductions to workshops".

It is possible that objectives for the workshop were discussed in detail in some workshops and only briefly in others. This is always a risk where workshops are repeated for different groups of participants. Further clarity of objectives was not requested during any of the workshops, however, a more frequent visitation of objectives and progress achieved towards those objectives may have been helpful for the participants. This may be of particular benefit to staff who have little or no knowledge of risk and security matters. Further investigation into the style of management meetings resulted in finding the hospital used an objective-oriented approach to management. That is, staff expect clearly defined objectives at the start of the meeting, and focus remains only on topics that relate directly to achieving those objectives.

One manager suggested that a discussion paper on topics to be covered in the meeting be distributed prior to the workshop. This may have been of assistance and would be worthwhile trying in future applications of the strategy. However, care must be taken not to structure the workshops too formally in content or process, as an essential element of the workshops is providing a supportive and expansive

environment for the free flow of ideas and views.

As it was difficult to get convenient times for all participants to meet, timing and duration of the workshops was an important consideration. Managers were given a month's notice to slot workshops into their schedules, and a choice of workshop times was given. The duration of each workshop was one hour, and the majority of attendees felt this was an acceptable length. As time was an important resource to managers, many commented how they appreciated the continued focus on the subject matter and keeping to the hour in the workshops.

The workshops appeared to flow easily through the planned content and all information was collated and distributed to staff promptly after each set of workshops. A valuable suggestion by two participants was to hold workshops concentrating on specific areas of information:

"Could have been improved by having 'specialist' workshops for speciality areas e.g. security of medical records with workshops for medical records staff".

"Need workshops for specific groups".

This suggestion was actioned and smaller meetings were held to discuss procedures and protective measures that related to each of the more sensitive types of information. These meetings were instrumental in designing the final procedures and security measures implemented to protect the most sensitive patient and hospital information.

8.2.1.3 Information Security and User Action

Although the staff at the hospital who participated in this research were not knowledgeable about specific security measures available, many interesting and unique ideas were put forward in a bid to solve some of the hospital's security concerns. A collection of comments relating to suggested solutions appear below. These comments were taken from the questionnaires completed by the participants during the workshops to discuss solutions. Focus by the staff appeared to

concentrate in three main areas, information security policies, written procedures, and ensuring the confidentiality of information. Security education was a major concern overlapping these three areas.

8.2.1.3.1 Security Policy

It appears that managers felt a detailed security policy needed to be developed and all staff be made cognisant of its contents. Also reflected was the desire to raise staff awareness at all levels regarding security issues and commitment to support protective measures put into place.

"The development of a security policy is the highest priority. It should form part of an overall information policy, incorporating a classification of information and access policy."

"A policy restates, clarifies, compliments and reminds all staff of their obligations to promote security within the hospital."

"A security policy needs to be clear and plain and needs to be signed off as an indication that it has been read and understood."

"The security policy needs to cover all personnel, including Doctors. Cleaners also need to be aware."

"The security policy needs to be more specific and detailed."

8.2.1.3.2 Written Security Procedures and Education

Support for written security procedures and guidelines is apparent, and the need for education was also recognised by many of the participants. The suggestions of security education as part of new staff orientation, and reminders regularly thereafter show a desire for an ongoing awareness of security matters. The breadth of staff

involvement in security education is also an important consideration reflected by the comments.

"Written procedures would be helpful. At times staff do not know what they should do."

"Definite guidelines to follow are needed."

"Education on the security procedures in relation to the different areas and security problems is very important."

"Raised awareness is the most important way of ensuring confidentiality. There needs to be continual reminders and encouragement."

"Education will assist with implementing all other suggested solutions - therefore should be done on orientation and followed up regularly."

"A friendly way of educating can be published in the newsletter, e.g. remember to log off when PC is not in use, etc."

"Security education should be an ongoing thing."

"Education is necessary on both the sensitivity of data and also the importance of integrity of data."

"Security education is needed with emphasis on using the formal communications channels, for effective information flow and transfer. This whole area needs strategies."

"The only way to get security education to work is to get it all together - it should be as compulsory as CPR and Manual Handling for all staff in the organisation."

"Security education is a high priority, particularly for Doctors. Staff should also be made aware of disciplinary action if confidentiality is breached."

8.2.1.3.3 Confidentiality of Information

The handling of confidential material was discussed at length in the workshops and comments indicate the need to revise the hospital's current confidentiality agreement. A further area of importance in considerations of confidentiality was the restriction of access to sensitive information to only those staff members with authority.

"I think all staff should sign a confidentiality agreement that also states they have attended the education course on security and confidentiality."

"The signing of a confidentiality agreement may be relevant to some groups, probably not doctors as this would cause more problems than it would solve."

"The current confidentiality agreement is unenforceable. It needs to indicate disciplinary action."

"Access to confidential information should be limited to managers only."

"Restricted computer access is important but hard to manage. Requires hard work."

The use of shredders to destroy sensitive material was discussed as a means of minimising the exposure of information leakage. It was generally agreed in workshops that shredders should be distributed throughout the hospital with concentration in areas dealing with confidential information. Comments relating to this area included:

"I don't think shredders will make any difference to security."

"Shredders should be put in areas of high confidentiality."

"Shredders are vital and they will also reduce the amount of gossip."

"Paper for shredding should stay in a box on the ward for at least one week before being transported to shredders."

"Information should be shredded immediately and not accumulated to be shredded at the end of the day. It should not be transported somewhere else to be shredded."

"Shredders are cheap and many could then be personally responsible for shredding their own stuff."

The above comments indicate that although the staff may not be knowledgeable about the technical aspects of specific security measures, there is an awareness of the importance of, and need for, many security solutions. At later stages in the research, it was the users who viewed the technical specifications of possible security solutions. After identifying the implications of potential solutions, the users again decided upon the most satisfactory measures to apply. With the aid of specialists where necessary, the staff themselves also installed or implemented the chosen security measures and redesigned hospital procedures around those solutions. This was a conscious action on the part of management as it was felt this would increase ownership and responsibility and assist the introduction of security into daily routine considerations.

This high level of involvement by users in the design and implementation of protective measures suggests that users can be highly aware of needs and required action to fill those needs. This indicates that information security may not be too technical for users to handle where specific security knowledge or guidance is provided.

8.2.2 FINDINGS RELATING TO THE PROCESS

8.2.2.1 User Involvement

Contribution levels by managers attending the workshops were high and there was good interaction between participants. A much broader view was developed due to

the varied areas of responsibility represented in each workshop group. This allowed participants to see a bigger picture, and appreciate the flows and integration of different areas. The impact of security problems across the organisation was more evident. In addition, managers were able to dove-tail solutions to enable other areas to be supported rather than hindered. For example, the records management system was very time-consuming to design and implement, but by careful analysis and planning, the final system assists all users of the information. Although strict procedures were implemented as part of this project, the access to information is clearly defined, and guidelines have been developed for the life of the information. This makes the management of the creation, modification, transportation, storage and destruction of documents (both computerised and hard-copy) more secure over the entire organisation.

The staff participating in the study were asked to rate how much involvement they believed staff should have in the security planning process. A summary of the responses is contained in Table 8.2. The results illustrate a high desire to involve staff in the ongoing planning and management of security, i.e. 94% of participants stating there should be either a high or very high staff involvement.

Question	1 Very Low %	2 Low %	3 Medium %	4 High %	5 Very High %
Desired Staff Involvement in Security Planning	0	0	6	76	18

Table 8.2: Desire by Staff to be Involved in Information Security Planning

This was in direct contrast to the view held at the beginning of the research. Before the first session commenced, the Director of Nursing stated, "I don't know why I have been invited to this seminar. My job has nothing to do with security." This same executive subsequently volunteered to be on the security task force established to implement the chosen security measures.

The desire to be part of the ongoing planning and management process was also reflected in some of the comments submitted by participants on the final questionnaire, including:

"Workshops needed compulsory participation of all recommended staff members".

"Some relevant people may have been excluded. Suggest attendance not by invitation only, but also by self-defined appropriateness".

It would appear there was enthusiasm by staff to be involved and a desire to continue to be involved, and that the breadth of participants be expanded to include other staff members.

8.2.2.2 Reflections On The Methodology

In action research learning takes place through reflecting upon action. Hence significant learning and building has eventuated by reflecting upon the application of the methodology and the model at the centre of this research. As seen in the previous chapter the use of SSM as a basis for the Orion Strategy caused some concern during the practical application of the model. The use of root definitions and conceptual models has also been seen to limit the usefulness of SSM by other practitioners (Hirschheim, Klein and Lyytinen 1995; Ledington and Ledington 1999). The concept of 'systems thinking' was difficult to apply because security measures protect the input, processing and output of other systems (i.e. information systems). Information security is contextual in nature and difficult to view as a system in itself. It follows, then, that CATWOE's, root definitions and conceptual modelling tools have limited application in a contextual environment, and these have been replaced by other analysis tools. (An entirely separate issue was the indifference of participants to rich pictures. Although rich pictures were used by the researcher as an aid for analysis during the entire process, the participants did not warm to this tool.)

As SSM is 'systems' based and this study is contextual in nature it is possible that

another methodology may have been more appropriate to use as a foundation. However, in essence, SSM was a reasonable choice. It is designed for high levels of user participation and interaction, and uses a shift in paradigm to tap into a creative element for finding the ideal situation. This shift in paradigm is a key concept in Dick's generic view of SSM (see Figure 6.2) and is worthy of consideration in this analysis of the Orion Strategy. Dick's interpretation of SSM is not 'system' based but 'dialectic' based, allowing the essence of SSM to be more easily applied to non-system situations (Dick, 1993).

A dialectic is "a process of change that results from an interplay between opposite tendencies" (MacQuarie Encyclopedic Dictionary, 1990:255). Dick describes each square in Figure 6.2 as a 'form of activity' or 'pole' (opposite tendency) and the ovals represent dialectics (process of change resulting from interplay). However, this model becomes more meaningful in the context of the Orion Strategy if the squares are viewed as static paradigms, or states of thinking, and the ovals as paradigm shifts into different states (see Figure 8.1).

In the context of this research the word 'paradigm' is used as it was redefined by Kuhn (1970), that is, a fundamental model of reality, and a 'paradigm shift' is a movement from one fundamental model of reality to another. When considering these squares as states of thinking, "*immersion in reality*" becomes the state of "*reality*"; "*define the essence*" becomes the state of "*essence*"; "*invent an ideal*" becomes the state of "*ideal*"; and "*proposed changes*" becomes the state of "*change*".

A paradigm shift is achieved by a change in perspective or consciousness, allowing the move to a different state to take place. The movement between different states is a two-way process, with revisitation of any state allowed as many times as required until a satisfactory outcome is reached.

Using this model for analysis of the Orion Strategy, the move from one state to another must be achieved in order to fulfil the activities in the Orion model (see Figure 8.2). That is, to fulfil the security actions contained within the ovals or spheres, there must be an immersion in each state of thinking and then a change of

focus to shift from one state of thinking to another.

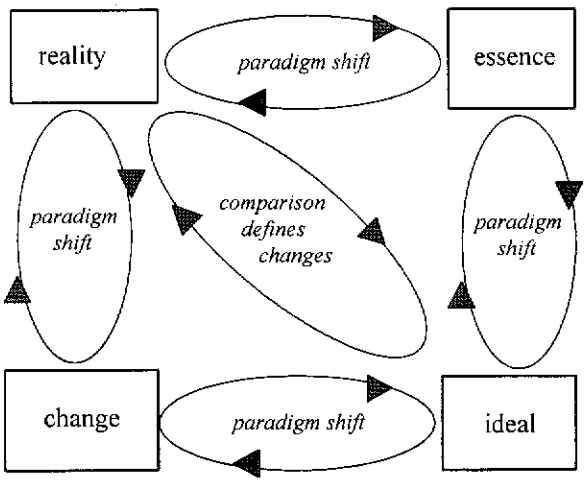

Figure 8.1 States of Thinking and Paradigm Shifts

For example, to define the ideal security situation it is necessary to move from thinking about the goal of securing the organisation's information in its essence, to a virtual reality of idealism. The action to build an ideal scenario can then be undertaken whilst within this ideal state of thinking.

Extending this concept further it could be suggested that these four states of thinking or realities are not separate but exist side by side, forming four quadrants of a complete matrix. This composite back-drop is static in nature. The paradigm shifts between these realities are dynamic, flowing between the different states (see Figure 8.3). Each set of activities contained within an oval requires thinking in at least one state, but usually two. A switch between the two adjacent states will be necessary to successfully complete most of the activities.

In the practical application of the Orion Strategy there was a constant revisiting of current reality, essence and the ideal states whilst analysing security needs and synthesising solutions. The flow allowing revisitation is represented by the circle containing two arrows appearing in the centre of the diagram in Figure 8.3.

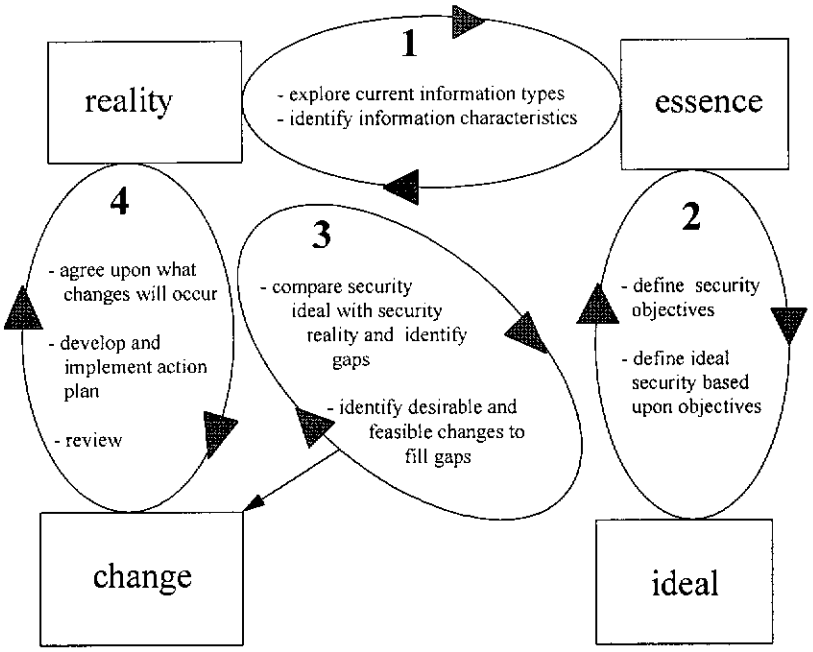

Figure 8.2: The Orion Strategy within States and Paradigm Shifts

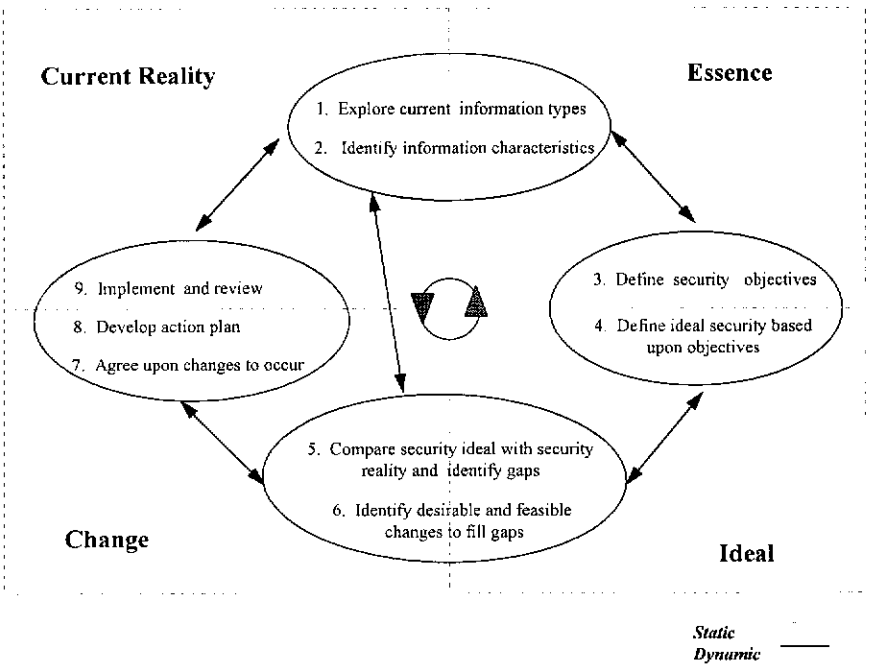

Figure 8.3: The Orion Strategy with States of Thinking

Viewing the activities within the Orion Strategy within the matrix of these four states allows more meaningful analysis of the contextual elements of the information security situation. The fluidity and ease of movement to and fro between the different states is also more accurately represented by the practical experience of its application at the hospital. The subsequent Orion model illustrated in Figure 8.3 above is hence more advanced and robust than the purely theoretical model originally presented in Chapter 6.

8.2.2.3 Reflections on Action Research

The use of action research as the mode for implementing the Orion Strategy was rewarding as it resulted in both research and action outcomes. The contribution to *research* has been the active building of a strategy that managers can use in the planning and ongoing management of information security. This approach was designed in detail as it was applied, merging the theoretical and practical aspects of the research.

The *action* component produced a plan for implementation of security solutions within the organisation. Solutions were evaluated and designed by the staff and implemented to improve information security throughout the hospital. Due to the high level of user involvement in the project the participants have undergone a learning experience. Participants claim their learning included more awareness about:

- activities within their own hospital and how these interact
- the types of information used within the hospital and the importance of this information
- the risks surrounding information and the need for its integrity, confidentiality and availability
- accepting responsibility for the information used in their daily work practices.

The involvement of key stakeholders their co-operation in applying solutions fulfils the participatory and collaborative elements that Kemmis and McTaggart (1988)

claim to be essential to the action research approach.

The cycles of action research were applied in several different forms. The overall Orion Strategy was applied only once, due to the size of the project and the three year time period of the research at the hospital. Figure 8.4 illustrates the *process* of the action research cycles and Figure 8.5 shows the *content* over the entire research project. In Figure 8.4 the planning stage for the entire project involved clarifying the research task and identifying those steps necessary to carry out that task. The action and observation stage put the plan into action by developing collaborative security solutions via workshops with users. The reflection stage reviewed the Orion Strategy and how it was applied, resulting in constructive feedback for future research planning.

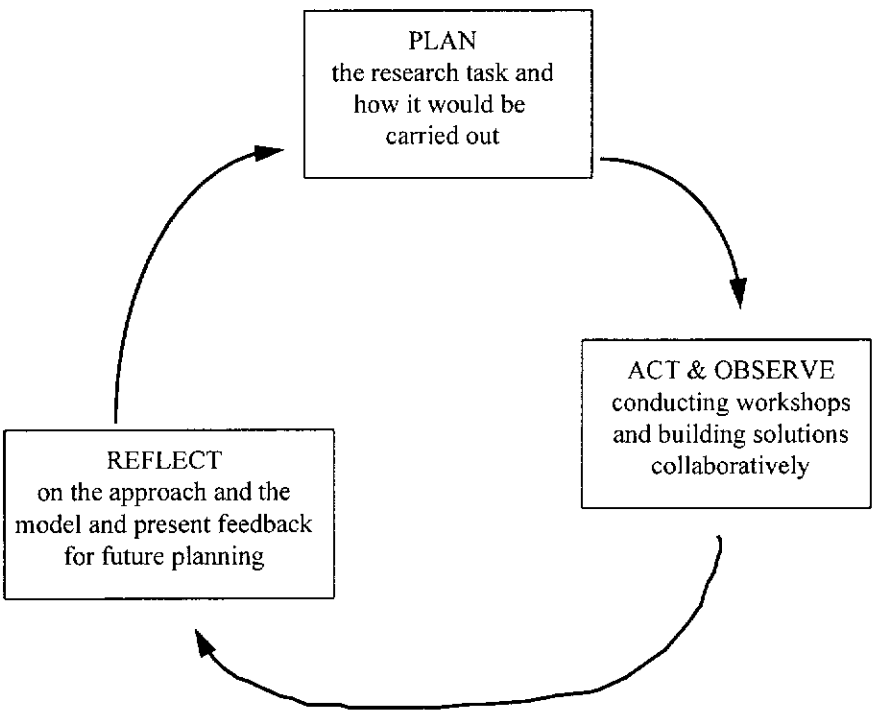

Figure 8.4 Action Research Cycle and the Process of the Research

The action research cycle relating to the content of the research (see Figure 8.5) is slightly different. The planning stage defined the necessary content and integration of each step of the process in order to achieve the research goal. The act and observe stage involved conducting workshops to define risks and solutions, undertaking a security review of the organisation and also implementing preferred solutions.

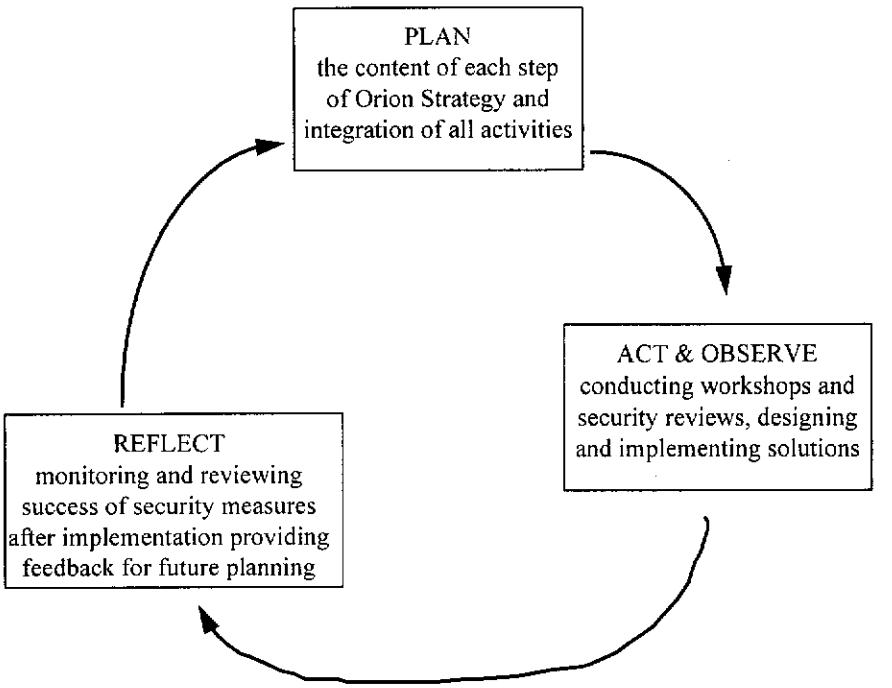

Figure 8.5 Action Research Cycle and the Content of the Research

During the reflection stage the success of security solutions is reviewed after their implementation to provide feedback for future planning and action. The reflection stage of the content is still going on within the hospital and will continue to do so, for as long as the agreed solutions are being implemented.

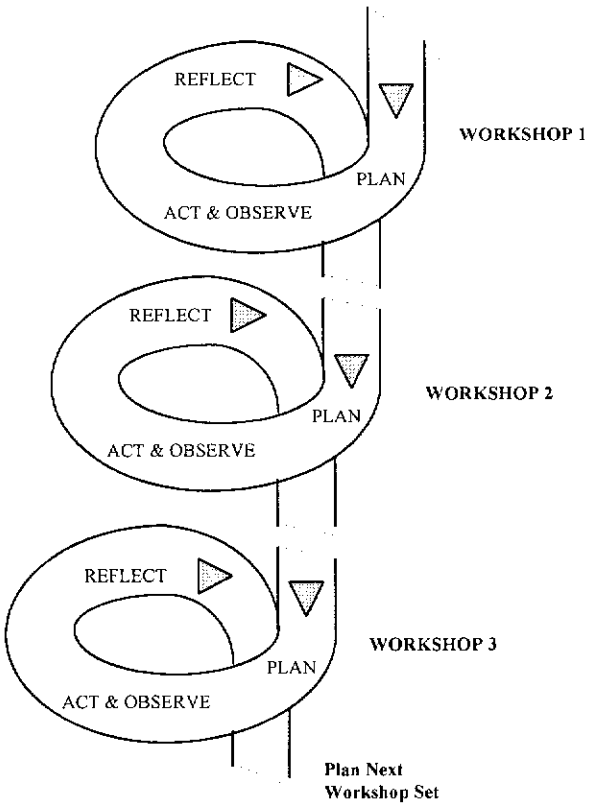

Figure 8.6 The Spiral Action Research Process of Each Workshop Set

Within the overall action research cycle, there were smaller cycles taking place during the workshop phases of the research. Workshops were held to address four major topics - risk analysis, information analysis, security ideals and analysing solutions. Due to the large number of participants three separate workshops were held for each topic, the three workshops combining to form a set. The action research cycle was performed both within each set, as well as over the four sets completed.

Within each set the content and process was planned before commencement of the first workshop. Following the workshop with the first group, these were reviewed by the facilitator, researcher and IS Manager. This review provided feedback for the improvement of the second workshop, and a similar process was carried out for the third workshop. Hence the action research cycle was performed three times for each workshop topic, or set of workshops (see Figure 8.6).

A similar procedure was carried out for sets of workshops. Reflection at the

completion of the risk analysis workshops set provided feedback for the planning of the workshops on information analysis (see Figure 8.7).

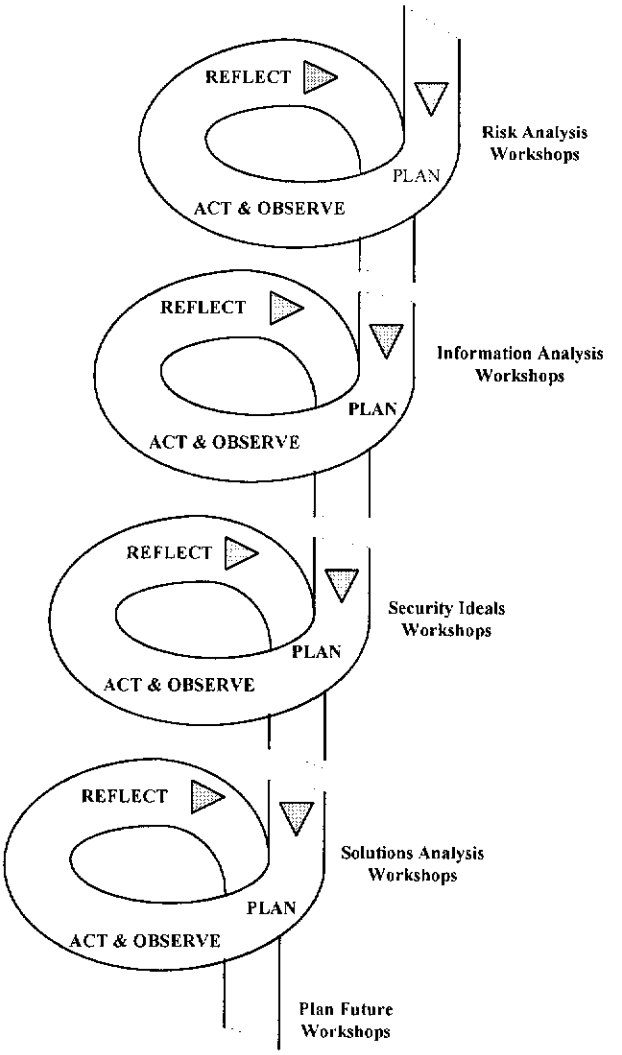

Figure 8.7 The Spiral Action Research Process of All Workshop Sets

Reflection was undertaken at the completion of each set of workshops, aiding the planning for the next set. This cyclical activity allowed a constant refining of the content and process of workshops as the research progressed, thus contributing to both the action outcomes as well as the research process.

8.3 LIMITATIONS

8.3.1 Bias in Data Collection

The possibility of bias in the conduct and interpretation of data collected from interviews, observations and questionnaires is acknowledged. However, action research is a subjective research approach and an objective interpretation was not sought. Wherever possible triangulation of methods utilising multiple data collection methods and collectors was employed to increase validity and reliability. For example, notes were taken by three individuals during the workshops and then combined at the conclusion of each workshop. In addition, information collected during the workshops was then confirmed by the questionnaires completed by participants at several stages of the research.

8.3.2 One Organisation, One Industry

The application of the Orion Strategy to only one organisation limits the generalisability of the findings. However, as the main aim of the research was to improve security management within the organisation in question, generalisable conclusions were not sought. Further research applying the strategy to other organisations, and also other industries is necessary before more global conclusions can be offered.

8.3.3 Participative Methodology

The staff involved were accustomed to participative approaches to management. Had the hospital not been familiar with participative methods the results could have been different. Within the hospital there appeared to be an accepted goal of reaching a solution and developing a plan of action before retirement from the task. Middle and senior managers also illustrated a unified desire to fulfil the organisation's overall mission. Political power struggles and hidden agendas were not apparent in the workshops or from interviews, and although there appeared to be a healthy respect for rank, in general there was open discussion and challenging of views.

It is recognised that similar conclusions could have been achieved via different methods, and that the Orion Strategy is only one potential means of successfully reaching the given aims. It may be possible that any highly participative planning framework could have resulted in a similar rise in security awareness and commitment by staff. However, any alternate method would need to support the basic activities of risk analysis, reviewing the current physical and logical security environment, determining the essence of the information security needs and evaluating and implementing appropriate security measures. Further research using different approaches is thus recommended.

8.3.4 Extent of User Involvement

The time and impact constraints on the research restricted user involvement to only sixty managers. A greater breadth could have been achieved by including all levels of staff, not just managers, however, this was not practicable. The limitation of participation to middle and senior managers with a stakeholding in the organisation's information was necessary in order to complete the research within the given time frame. In the ideal situation all employees at all levels would be involved in the entire process, as all information users are stakeholders in some form.

8.3.5 Workshop Facilitation

The conventional methods of security management involve security reviews and recommendations by security specialists. In order to reduce the influence of the researcher's preconceived notions of security risks and solutions, an independent facilitator was used in the workshops. This facilitator was familiar with the health care industry and understood the terminology used. The researcher acted only as an observer and security adviser during the workshops, thus encouraging staff to create their own solutions, to risks they themselves had identified.

However, the researcher was able to suggest potential security measures that may have been appropriate for the areas of vulnerability identified. Although independent

advice was sought by the hospital's security task force, it is recognised that the researcher's recommendations may have biased the subsequent choice of measures.

8.4 CHAPTER CONCLUSION

The study showed an improvement in the application and supervision of information security at the hospital over the period of the research. The high level of user involvement resulted in the staff themselves identifying areas of risk and suggesting solutions to minimise the related exposure. With a little guidance, the staff themselves designed procedures, evaluated security products and implemented a variety of security measures in their workplace.

It was generally felt by a large majority of the participants that staff involvement in security planning and management in the future should be high and that a greater proportion of the staff be included.

Reflections on the use of the model resulted in a revisitation of the Orion Strategy based upon Dick's (1993) generic view of SSM, rather than the Checkland (1981) model. The Orion Strategy has been redesigned to include different states of thinking and the process of paradigm shifts to move between these states. These changes have allowed more meaningful analysis of the context within which the model's activities took place.

Action research was carried out at several levels. The overall research was undertaken within one action research cycle. At a lower level, the action research cycle was repeated several times during the workshop phases of the research. The use of action research resulted in both positive research and action outcomes. The application of the Orion Strategy resulted in a practical model that can be applied to future research. The action outcome was a practical plan for the implementation and subsequent management of preferred security measures in the hospital environment.

9 EMERGING THEMES and CONTINUITY OF RESEARCH

9.1 CHAPTER INTRODUCTION

This chapter discusses emerging themes arising from the research in addition to the findings discussed in the previous chapter. The first theme evident relates to the acceptance of ownership of the chosen security measures and the second to the increased awareness claimed by participants regarding information security issues. Possible areas of future research related to the work undertaken herein are considered. These areas cover potential research on the methodology as well as the type and breadth of possible participant organisations. The chapter concludes with a discussion of the implications of this research.

9.2 EMERGING THEMES

9.2.1 Ownership of Information Security

As discovered in the discussion within Chapter 2 there is a generally held view that information security is the responsibility of the IS Department, and this was also the belief at the hospital participating in this research. One of the managers at the hospital commented just prior to the initial education seminar "information security is not my responsibility, it is the responsibility of our IS Department. I think this seminar will be a waste of time for me". The IS Manager at the hospital confirmed this view was common throughout the hospital.

Responsibility for information security was one of the topics covered in the initial education seminar, and the difference between ownership and custodianship of corporate information explained. The users "own" their information, and the IS Department is the "custodian" of that information whilst it is stored on the computer systems the IS staff manage. Within its life cycle, users create information from transactions within their areas of work and this information is then entered into a computer system for future reference by the same or other users. In order for the IS people to store that information securely (as custodians of the information only), the users themselves must define its sensitivity and their requirements for its protection

and usage. The IS Department provides the services of sorting, formatting, processing and delivering this information back to users via enquiries and reports. Figure 9.1 illustrates this concept.

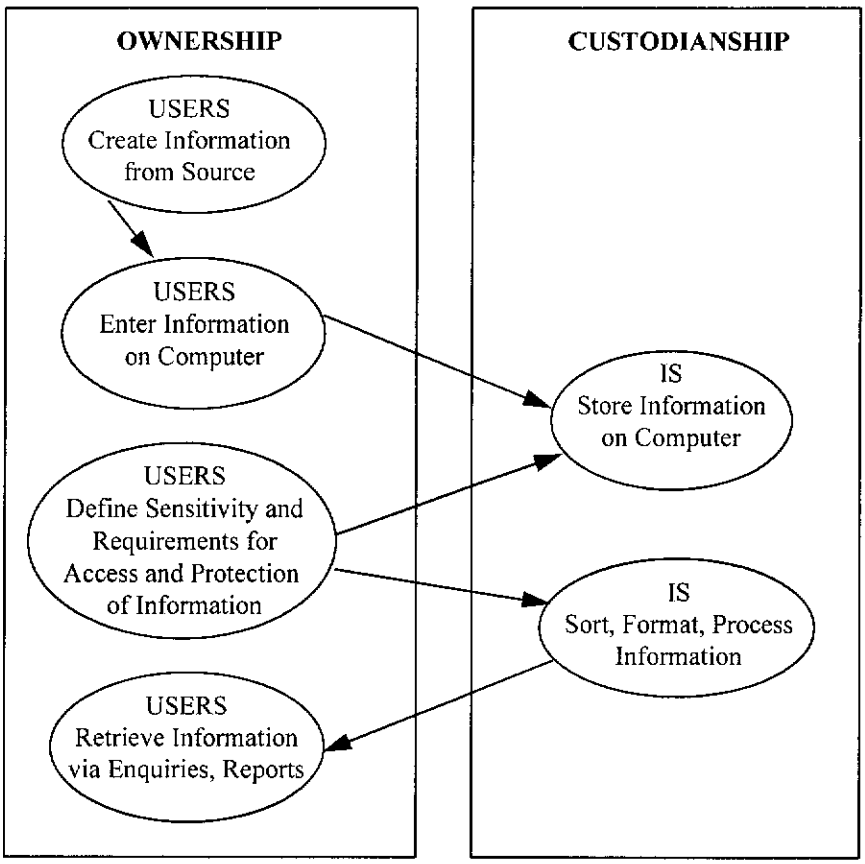

Figure 9.1: Ownership and Custodianship of Information

The education seminar explained the importance of the involvement of users in the security management process as information stakeholders. This stakeholding also incorporated an acceptance of responsibility for the security of that information.

As planned, during the workshops the tasks of identifying risks and designing appropriate security measures were carried out by the staff themselves. This provided encouragement for the participants to take on ownership of the solutions

and accept responsibility for their ongoing management.

At the completion of the workshops the participants were asked to rate their level of acceptance of responsibility and ownership of the solutions implemented. Table 9.1 summarises their responses. Taking on the responsibility for security and owning the security measures was rated highly, with 94% rating their ownership at a high or very high level. These findings were also consistent with information collected via interviews with the participants.

Question	1 Very Low %	2 Low %	3 Medium %	4 High %	5 Very High %
Ownership of Responsibility for Security Measures	0	0	6	59	35

Table 9.1: Ratings by Participants relating to Ownership of Security Measures

For example, one manager stated

"We are like security radars walking around the hospital. As we do our daily work we are always conscious of security needs".

Another participant stated on the questionnaire:

"Workshops were excellent as it brought all parties together. We were able to discuss real problems and reasonable and effective solutions were discussed and implemented".

The continuing implementation of agreed security measures was managed by a volunteer six-person task force. Responsibility for the chosen security measures was distributed and handed over to the staff responsible for the safekeeping of the asset in

question. As the participants in the study were senior management, there was excellent support and drive for the complete implementation of those security solutions.

9.2.2 Awareness of Security Issues

One of the problems arising from the background research discussed in Chapter 2 was the poor level of awareness regarding risks and possible security solutions. By using a high level of user involvement in the planning and management of information security at the hospital it was hoped that participants would become more aware of security issues. In particular the initial education seminar was designed to increase knowledge about potential risks and the importance of effective security management. In addition, the workshops were designed to walk the participants through risk identification within their own working environment and devise appropriate solutions to support the hospital's mission and goals.

In order to measure how effective the education seminar and workshops had been participants were asked to rate their awareness of security issues at three stages throughout the planning project: before it began, after the security education seminar, and finally at the end of the workshops. These three ratings were all completed at the end of the workshops.

The responses are shown in Table 9.2. A notable shift in awareness is indicated as a result of the initial education seminar, with all respondents claiming a rise in the level of awareness after attending the seminar.

Questions relating to Awareness	1 Very Low %	2 Low %	3 Medium %	4 High %	5 Very High %
Security Awareness Before Project Began	0	18	41	41	0
Security Awareness After Education Seminar	0	0	29	41	30
Security Awareness After Risk and Solution Workshops	0	0	0	41	59

Table 9.2: Ratings of Security Awareness over the Research Period

A senior executive attending the seminar made the following comment on the questionnaire:

"Great initiative - important topic which will be supported by Executive".

These workshops were highly participative, with users willingly becoming involved in the problem identification and formulation of solutions. The discussion within the workshops was driven by the groups themselves, with the facilitator acting solely as a guide.

A similar rise in levels of awareness were noted after the workshops were completed, with all participants claiming a high or very high level of awareness. Comments made on the questionnaire regarding the workshops include:

"Workshops were enlightening and relevant. The issues raised certainly heighten concerns that were already held".

"The workshops have increased awareness at a personal level. I am now particularly interested in the policy development and education of staff".

"The workshops were very valuable for people making decisions together".

"Contribution was good and participation in our group was good".

"Interactive format was an excellent way to encourage discussion and the way I learn best".

"Excellent facilitation, hearing points of view, plus collation and feedback".

"Education regarding information management procedures including security measures and procedures would fit into the context of a policy and plan. This would emphasise the positive benefits of correct use of information - we all need it in our work. We should be trying to ensure access to those who need it, to correct, authoritative information".

However, one participant appeared to be concerned that fellow staff members would react from fear following the education seminar as illustrated by this comment on the questionnaire.

"Isolated as an issue, information security is sensationalised, and although I think the need is real, I think the 'knee jerk' response will come from fear rather than as part of a reasoned decision making process and viewed in perspective".

The feedback given in the ratings and comments was helpful in determining the usefulness of the education seminar and workshops as tools for carrying out the activities of the Orion Strategy. It appears that staff generally found the seminar and workshops of benefit, raising their awareness of security issues and encouraging ownership of chosen protective measures.

9.3 FUTURE RESEARCH AREAS

The broad aim of the research was to improve information security management within a given organisation. The current state of play in theory and practice has been reviewed and a new model developed to address the emergent gaps. This new model was based upon a proven theoretical methodology; then developed further as it was

implemented. The path chosen for this research was only one of many alternatives. The base methodology could have been different, as could the type of organisation involved in the application of the model. These two factors, plus others, are now discussed as options for future research.

9.3.1 Different Methodologies

The problem solving methodology used as a foundation for this research was SSM and it was implemented using the action research method. SSM is only one problem solving methodology incorporating a high level of user participation. Other methodologies could be applied to the topic area with the aim of improving the management of information security. Methodologies proven in other disciplines could be adapted and used in the information security environment to determine their applicability. In addition, a number of different methodologies could be employed and the results compared to determine the best methodological fit.

The attempt to match SSM (a methodology centered upon *systems* thinking), with information security management (a *contextual* matter), resulted in having to adapt the tools and techniques to suit the given research situation. Viewing information security as a system in itself proved difficult in the context of this research. Perhaps other problem solving methodologies would have been more suitable. A study to identify alternate appropriate methodologies could be beneficial.

In addition, the application of the reviewed Orion Strategy illustrated in Figure 8.3 could be undertaken to determine whether this revised version is able to be applied, and how well it can be adapted to a given organisational situation.

Action research is the research method or tool commonly utilised to implement SSM. The use of an alternate research method could also be entertained. However, the choice of such a method would need to complement and support the problem solving methodology used.

9.3.2 Different Organisations for Practical Application

Future research in this area could include the application of the Orion Strategy in one or more health care organisations. The level of implementation of information security measures over the period of the project, as well as the level of stakeholder ownership, could then be compared with the results of this research. This would allow a more comprehensive view of the applicability of the Orion Strategy within the health care industry.

Alternatively, the Orion Strategy could be implemented within organisations in industries other than health care. The level of implementation of information security measures within differing industries could be studied. Ownership by stakeholders could also be studied within organisations existing in different industries.

9.3.3 Inclusion of Wide Area Networking and Internet Considerations

Extension of the study to include considerations relating to telecommunications would also be of benefit to organisations utilising global networking and the Internet. The principles applying to the security of information to wide area networks are similar to those for the Internet. Information is the commodity that drives the Internet and protection of corporate information is at risk once corporate computer systems are connected. Research in this area would be highly beneficial to organisations relying upon telecommunications as a core part of their organisational strategies.

9.3.4 Information Security Auditing

The Orion Strategy has the ability to be used as an adjunct audit tool. With the aim of improving the management of information security, auditors could employ this technique to organisations requiring increased user awareness and ownership of security responsibility. An area of future research could be comparisons of audit status with one or more organisations before and after employing the Orion Strategy

to measure any change.

9.3.5 The Learning Organisation

The experiences noted by the researcher, the facilitator and the IS Manager at the hospital site, agreed that the project had resulted in a huge learning situation for those involved. This learning experience was likened to that of a 'learning organisation". The essence of the learning organisation is "metanoia" which means a shift of mind, as learning also encompasses a fundamental shift or movement of mind (Senge 1992). This is achieved by team thinking, and true team learning commences with dialogue, where the members of the team are able to let go of assumptions and enter into genuine collective thinking.

The main elements of a learning organisation are systems thinking, personal mastery, mental models, building a shared vision and team learning (Senge 1992). The study of information security management within a learning organisation is an area of possible future research. A systems thinking and highly participative approach, such as SSM, would be necessary to ensure the metanoia resulted from collective thinking and team learning.

9.4 CONCLUSION

To summarise briefly, this research centers upon the management of information security with the aim of developing effective practices to ensure information integrity, confidentiality and availability. The activities undertaken as part of this research commenced with a study of current literature on the state of computer abuse and security management. It was previously reported in Chapter 2 that information security management was poor in many parts of the world. Sixty Australian organisations were then investigated to determine the current level of implementation of recommended security measures to protect corporate information. Analysis of the findings of that investigation are discussed in Chapter 4 reporting in a general lack of implementation of security measures across organisations, with the health care industry illustrating particularly poor ratings. Consistently apparent was a lack of user involvement in security issues, with users having little awareness of areas of

vulnerability or how and why security measures were implemented. A common belief has been that security is a technical issue and therefore an IS Department responsibility.

A search for methodologies and approaches to assist managers increase the level of effective protective measures to secure corporate information was completed. An approach incorporating a higher level of user involvement was searched for, however the models presented in the literature were predominantly technical or academic in nature with little evidence of practical application (see Chapter 5). This section of the research identified a variety of models and approaches, however, there was no one approach identified to fill the apparent need.

In line with these findings this thesis has presented an alternative approach to contemporary information systems practice, the Orion Strategy. This approach has a high level of stakeholder participation and aims to encourage information stakeholders to take responsibility for the information within their work areas. The building of the Orion Strategy was a move towards a greater user involvement in the planning and management of information security (see Chapter 6). The application of the Orion Strategy at a private hospital has been a learning process, and as discussed in Chapter 7 the model was honed and further developed as it was used.

Feedback on the use of the Orion Strategy at the hospital site has been positive, with several significant outcomes. The first achievement was an increase in the ratings for implementation of security measures over the period of the project. The second was the increased level of ownership of responsibility by staff for the security of information in their work environment.

Additional findings included an increase in the awareness of security issues by staff, and their willingness to be involved in the ongoing planning and management of information security within the hospital.

The results of this research encourage security specialists, auditors and managers to continue in the quest to empower users to accept and own the responsibility for information security planning and management.

REFERENCES

Anonymous, 1997, "Maximum Security: A Hacker's Guide to Protecting your Internet Site and Network", Samsnet, Indiana, USA

Abrams, M.D. & Moffett, J.D. 1995, 'A Higher Level of Computer Security Through Active Policies', *Computers & Security*, vol.14, no. 2, pp. 147-157

Abrams, M.D., & Zelkowitz, M.V., 1995, 'Striving for Correctness', *Computers & Security*, Vol. 14, No. 8, pp 719-738

Adams, J. 1995, 'Internal Losses: Controlling and Investigating Corporate Crime', *Security Australia*, August, pp 22-23

Alexander, M. 1995, 'The Real Security Threat: The Enemy Within', *Datamation*, July 15, pp 30-33

Alexander, M., 1996, "The Underground Guide to Computer Security", Addison-Wesley, Reading Massachusetts, USA

Allen, R., 1995, 'The Path to Excellence for Information Technology Organisations', *IS Audit & Control Journal*, vol.1, pp32-34

Anderson, A., Longley, D., Tickle, A. 1993, 'The Risk Data Repository: A Novel Approach to Security Risk Monitoring', in *Computer Security*, Ed E. Dougall, Elsevier Science Publishers, North-Holland

Anderson, E. 1985, 'Managerial Considerations in Participative Design of MIS/DSS', *Information & Management*, vol. 9, pp 201-207

Anderson, J. 1972, 'Information Security in a Multi-user Computer', in *Advanced Computers*, Ed Rubinoff, Academic Press, New York

Anderson, J.G., 1997, "Clearing the Way for Physicians' use of Clinical Information Systems", *Communications of the ACM*, Vol. 40, No. 8, pp 83-90

Angell, I.O. 1993, 'Computer Security in These Uncertain Times: The Need for a New Approach', *Proceedings of the tenth world conference on Computer Security, Audit and Control, COMPSEC 93, London*, Elsevier Advanced Technology, North Holland, pp 382-388

Angell, I. 1995a, 'Security, the Core of the Modern Enterprise', *Forum*, February, p10

Angell, I. 1995b, 'Security is a Growth Industry', *Forum*, August, 2, p 6

Annas, G., 1993, 'Privacy Rules for DNA Databanks: Protecting Coded "Future Diaries", *Journal of American Medical Association*, vol. 270, pp 2346-2350

Antill, L., 1985, 'Selection of a Research Method', in Mumford, Hirschheim, Fitzgerald & Wood-Harper (eds), '*Research Methods in Information Systems*', North-Holland, Netherlands, pp 203-218

Arbouw, J. 1993, 'Crimes and Misdemeanours', *Australian Business Monthly*, March, pp 31-32

Argyris, C., Putnam, R., & Smith, D.McL, (1985) '*Action Science - Concepts, Methods and Skills for Research and Intervention*', Jossey-Bass, San Francisco, USA

Avison, D. and Fitzgerald, G., 1995, *'Information Systems Development: Methodologies, Techniques and Tools'*, McGraw-Hill, London

Avison, D. and Wood-Harper, T., 1990, *'Multiview: An Exploration in Information Systems Development'*, McGraw-Hill, Maidenhead

Backhouse, J. & Dhillon, G. 1993, 'A Conceptual Framework for Secure Information Systems', *Proceedings of the tenth world conference on computer security, audit and control, COMPSEC '93, London*, Elsevier Advanced Technology, pp 158-168

Backhouse, J. & Dhillon, G. 1995, '*Working Towards Principles for Information Security Management in the 21st Century*', CSRC/95/3, Computer Security Research Centre, London School of Economics and Political Science, London UK

Badri, M.A. 1992, 'Critical Issues in Information Systems Management: An International Perspective', *International Journal of Information Management*, vol.12, pp 179-191

Baker, R.H., 1995, '*Network Security*', McGraw-Hill, New York

Bakker, A., van Dorp, H. & van Veenen, G., 1996, 'Guidelines for Secure System Development and Secure Implementation', in Barber, Treacher & Louwerse, (Eds), "*Towards Security in Medical Telematics*", IOS Press, Amsterdam, pp 184-189

Bakos, J.Y. & Treacy, M.E., 1986, 'Information Technology and Corporate Strategy: A Research Perspective', *MIS Quarterly*, June, pp 106-119

Barber, B. and Davey, J., 1992, 'The Use of the CCTA Risk Analysis and Management Methodology (CRAMM) in Health Information Systems', in Lun, Degoulet, Piemme & Rienhoff (Eds), "*MEDINFO 92*", North Holland, Amsterdam, pp 1589-1593

Barber B. and Davey, J., 1996, 'Risk Analysis in Health Care Establishments', in Barber, Treacher & Louwerse, (Eds), "*Towards Security in Medical Telematics*", IOS Press, Amsterdam, pp 120-124

Barber, B., Vincent, R. & Scholes, M., 1992, 'Worst Case Scenarios: The Legal and Ethical Imperative' in Richards, B. et al (Eds), "*HC92 Current Perspectives in Healthcare Computing*", 1992, British Journal of Healthcare Computing, pp 282-288

Baskerville, R., 1988, '*Designing Information Systems Security*', John Wiley & Sons, Chichester, UK

Baskerville, R., 1996, 'A Taxonomy for Analysing Hazards to Information Systems', in Katsikas S.K. & Gritzalis D. (Eds), '*Information Systems Security*', Chapman & Hall, London, pp 167-176

Baskerville, R., 1997a, 'Distinguishing Action Research from Participative Case Studies', *Journal of Systems and Information Technology,* vol. 1, no. 1, March, pp 25-45

Baskerville, R., 1997b, 'New Organisational Forms for Information Security Management', in Yngstrom, L. and Carlsen, J. (Ed's), *'Information Security in Research and Business'*, Chapman and Hall, London, pp 296-307

Baskerville, R. and Wood-Harper, A.T., 1996, 'A Critical Perspective on Action Research as a Method for Information Systems Research', *Journal of Information Technology*, vol.11, pp 235-246

Baskerville, R. and Wood-Harper, A.T., 1998, 'Diversity in Information Systems Action Research Methods', *European Journal of Information Systems*, vol.7, no. 2, June, pp 90-107

Bauknecht, K. & Strauss, C., 1991, 'Portfolio Techniques to Support Risk Management and Security', in *Computer Security and Information Integrity*, eds Dittrich, Rautakivi and Saari, Elsevier Science Publishers, North Holland

Bawden, R. & Zuber-Skerritt O., 1991, 'Learning, Process Management and Change', in *Action Learning for Improved Performance*, Ed Zuber-Skerritt, AEBIS Publishing, Brisbane, Australia

Becker, R.S. 1977, *'The Data Processing Security Game'*, Pergamon Press

Benbasat, I., Goldstein, D., Mead, M. 1987, 'The Case Research Strategy in Studies of Information Systems', *MIS Quarterly*, September, pp 369-386

Benbow, G., Masters, J., Cooper, B. 1986, '*Computer Security in Australia*', Royal Melbourne Institute of Technology Ltd, Australia

Bentley, D.F., Hinde, S.V. & Oliphant, A.S., 1995, '*Computer Audit and Control Handbook*', Butterworth Heinemann, UK

Benton, J., 1998, 'Physical IT Security', *Computers & Security,* vol. 17, no. 1, pp 389-391

Berleur, J., 1999, 'Self Regulation and Democracy: Choice and Limits', in Fischer-Hubner, Quirchmayr & Yngstrom, Eds, '*User Identification & Privacy Protection*', Proceedings of the Joint IFIP WG8.5 and WG9.6 Working Conference, Stockholm University, Sweden, pp 1-20

Bequai, A., 1998, 'High-Tech Security and the Failings of President Clinton's Commission on Critical Infrastructure Protection', *Computers & Security*, vol. 17, no. 1, pp 19-21

Bergman, J., 1991, Fundamentals of Computer Security and Risk Analysis, *Proceedings of EDPAC '91*, Canberra, May, pp 1-28

Bhaskar, K. (1993) '*Computer Security: Threats and Countermeasures*', NCC-Blackwell, Oxford, UK

Bjorn-Anderson, N. 1983, 'Challenge to Certainty', in *Beyond Productivity: Information Systems Development for Organisational Effectiveness, Ed* Bemelmans, North-Holland

Blair, G., 1991, 'Network Security', *Proceedings of the Third South Pacific Region Security Conference of ASIS*, July 16-18, Melbourne, pp 24-42

Bleumer, G., 1996, 'Cryptographic Mechanisms for Health Care IT Systems', in Barber, Treacher & Louwerse, (Eds), "*Towards Security in Medical Telematics*", IOS Press, Amsterdam, pp 233-237

Blobel, B., 1997, 'Security Requirements and Solutions in Distributed Electronic Health Records', in Yngstrom, L. and Carlsen, J. (Ed's), "Information Security in Research and Business", Chapman and Hall, London, pp 377-390

Blobel, B. and Pharow, P., 1999a, 'Data Protection in Healthcare and Welfare' in Yngstrom and Fischer-Hubner, (Ed's), '*WISE 1*', Proceedings of the IFIP TC11 WG11.8 First World Conference on Information Security Education, Stockholm University, pp 63-82

Blobel, B. and Pharow, P., 1999b, 'The Need and Practice of User Authentication and TTP Services in Distributed Health Information Systems', in Fischer-Hubner, Quirchmayr & Yngstrom, (Ed's), '*User Identification & Privacy Protection*', Proceedings of the Joint IFIP WG8.5 and WG9.6 Working Conference, Stockholm University, Sweden, pp 129-148

Boom R. 1990, "Software Quality Management", *Industrial Management and Data Systems,* Vol 90, No 3, pp 9-11

Bostrom R. and Heinen S. 1977, "MIS Problems and Failure: A Socio-Technical Perspective, Part 1: The Causes", *MIS Quarterly*, Vol 1, No 3, September, pp 17-32

Bourgeois, L. & Eisenhardt, K., 1988, 'Strategic Decision Processes in High Velocity Environments: Four Cases in the Microcomputer Industry', *Management Science*, vol. 34, pp 816-835

BSAA, 1989, '*Software Compliance Manual for Decision Makers*', BSA Software Australia Pty Ltd, New South Wales, Australia

Buckley F. and Poston R. 1984, "Software Quality Assurance" *IEEE Transactions on Software Engineering*, Vol 10, No 1, January pp 36-41

Burn J, Saxena K. Ma L, Cheung H, 1992, 'Critical Issues of IS Management in Hong Kong: A Cultural Comparison', *Journal of Global Information Management*, September, 1(4), pp 28-37

Cairo, L. & Friedberg, A., 1995, 'Security in Client/Server: Authentication Issues', *IS Audit & Control Journal,* vol.IV, pp 48-53

Cameron, J., 1993, 'Information Technology (IT) & Society: it Impacts!', *Proceedings of the Symposium on Virtual Ethics in the Age of Computing, Canberra, Australia*, March, pp 25-33

Carr, W. & Kemmis, S. 1986, '*Becoming Critical: Education, Knowledge and Action Research*', Falmer Press, London

Carroll, J.M., 1996, "*Computer Security*", Butterworths, Boston, Massachusetts, USA

Carroll, J., & MacIver, W., 1984, 'Towards an Expert System for Computer Facility Certification', in Finch, J. & Dougall, E. (Ed's), *Computer Security, A Global Challenge,* North-Holland, Amsterdam, pp 293-306

Chantico Publishing Company Inc., 1985, '*Disaster Recovery: Contingency Planning and Program Evaluation*', QED Information Sciences, Massachusetts

Chantico Publishing Company Inc., 1992, '*Combating Computer Crime*', McGraw-Hill, New York, USA

Chantler, A.N., 1989, 'Rogue Code', *Proceedings of the Second ACARB Conference*, Gold Coast, Queensland

Chantler, A.N., 1992, ' In Your Competitor's Shoes', *Australian Computer Society Seminar,* September 14, Perth, Western Australia

Checkland, P., 1981, '*Systems Thinking, Systems Practice*', John Wiley & Sons, Chichester, UK

Checkland, P., 1991, 'From Framework through Experience to Learning: the Essential Nature of Action Research', in '*Information Systems Research:*

Contemporary Approaches and emergent traditions', eds Nissen HE, Klein HK, & Hirschheim R, Elsevier, Amsterdam

Checkland, P. & Scholes, J., 1990, '*Soft Systems Methodology in Action'*, John Wiley & Sons, Chichester, UK

Cheswick, W.R. & Bellovin, S.M., 1994, '*Firewalls and Internet Security - Repelling the Wily Hacker'*, Addison-Wesley, Massachusetts

Chidley J. 1995, Cracking the Net, *MacLean's,* May 22, pp 54-56

Clay, B.M. 1995, 'PC Security Criteria A to Z', *IS Audit & Control Journal*, vol. V, pp 27-32

Clark, C. 1993, 'IBAG Framework for Commercial IT Security', in *Proceedings of COMPSEC, tenth world conference on Computer Security, Audit and Control, London,* October, Elsevier Science Publishers, North-Holland, pp 280-287

Clark R. 1989, 'Risk Management - A New Approach', in Grissonnanche A. (Ed) *Security and Protection in Information Systems*, Elsevier Science Publishers, North-Holland

Clough, B. and Mungo, P., 1992, '*Approaching Zero'*, Faber and Faber, London, UK

Cohen, F., 1992, 'Computer Viruses', in Jackson, K.M. & Hruska, J., 1992, '*Computer Security Reference Book'*, Butterworth Heinmann, Oxford, UK, pp 641-664

Collins B. & Mathews S. 1993, 'Securing Your Business Process', *Proceedings of the Tenth World Conference on Computer Security, Audit and Control*, COMPSEC '93, London, May, Elsevier Advanced Technology, pp 11-18

Cooper, F.J., Goggans, C., Halvey, J.K., Morgan, L., Siyan, K., Stallings, W. & Stephenson, P., 1995, '*Implementing Internet Security'*, New Riders, Indiana

Coopers and Lybrand, 1988, '*The Security of Network Systems'*, Coopers & Lybrand, USA

Corbeel, L., Corbeel, I. & Hortmann, M., 1996, 'Data Protection and Security within TANIT', in Barber, Treacher & Louwerse, (Eds), "*Towards Security in Medical Telematics"*, IOS Press, Amsterdam, pp 162-167

Corbin, D.S., 1991, 'From Nerd to Normal in 10 Easy Steps: A Guide for IS Pros', *Journal of Systems Management*, June, pp 32-34

Corby, M. and Johnston, R., 1998, 'Intranet Security Guidelines: How to Protect the Enterprise as Your Intranet Grows', *Computer Security Journal*, vol. XIV, no. 4, pp 1-6

Cordonnier, V. & Watson, A., 1998, 'Access Control Determination of Smart Cards using a Quantification of Security Levels', *Security Journal*, vol. 10, pp 89-95

Corrigan, P.H., 1994, '*LAN Disaster Prevention and Recovery*', Prentice-Hall, Englewood Cliffs, New Jersey

Council on Scientific Affairs, 1993, 'Confidential Health Services for Adolescents', *Journal of American Medical Association*, vol. 269, pp 1420-1424

Cowcher, R., 1992, 'Physical Security', in Jackson, K.M. & Hruska, J., 1992, '*Computer Security Reference Book*', Butterworth Heinmann, Oxford, UK, pp 311-331

Criminal Justice Commission, 1993, '*Corruption Prevention Manual*', CJC, Queensland

CSI Roundtable, 1998, 'Process for Handling Company Proprietary Information', *Computer Security Journal,* vol xiv, no. 2, pp 10-14

Curry, D.A., 1992, '*UNIX System Security*', Addison-Wesley, Reading Massachusetts, USA

Dacier, M., Deswarte, Y. & Kadniche, M., 1996, Models and Tools for Quantitative Assessment of Operational Security, in '*Information Systems Security*', Katsikas S.K. & Gritzalis D. (eds), Chapman & Hall, London

Damman, U., 1996, 'The Data Protection Commissioner's Point of View', in Barber, Treacher & Louwerse, (Eds), "*Towards Security in Medical Telematics*", IOS Press, Amsterdam, pp 81-82

Dampney C., Hansell A., Borthwick K. and Gilmour P., 1984, *'Directing Information Systems in an Organisation: What is Important and Why?'*, Joint International Symposium in Information Systems, Sydney, April 9-11

Darke, P., Shanks, G. & Broadbent, M., 1998, 'Successfully Completing Case Study Research: Combining Rigour, Relevance and pragmatism', *Information Systems Journal,* vol. 8, October, pp 273-289

Data Protection Act, 1984, '*The Guideline Series and Guidance Notes*', Office of the Data Protection Registrar, Willmslow, Cheshire

David J. 1995, 'Organisational Security - Clean Up or Cover Up?', *Computers & Security*, vol.14 no.2, pp 99-101

Davies, D. 1986, 'Confidentiality, Integrity, Continuity', *Computer Control Quarterly*, Spring, pp 28-31

Davies, L. and Ledington, P., 1991, '*Information in Action: Soft Systems Methodology*', Macmillan, London

Davis A. 1990, "System Testing: Implications of Requirements Specifications", *Information and Software Technology*, Vol 32, No 6, July/August, pp 407-414

Davis, P.T., 1994, '*Complete LAN Security and Control*', Windcrest/McGraw-Hill, New York

Deans C, Karwan K, Goslar M, Ricks D, Toyne B, 1991, 'Key International IS Issues in the US-based Multinational Corporations', *Journal of Management Information Systems*, 7(4), pp 27-50

Dietzel, G., 1996, 'The Commission's Expectations in Security', in Barber, Treacher & Louwerse, (Eds), "*Towards Security in Medical Telematics*", IOS Press, Amsterdam, pp 2-3

DeMaio A. 1980, "Socio-Technical Methods for Information Systems Design" in Lucas et al (Ed's) *'The Information Systems Environment'* North-Holland, pp 105-122

DeMaio H.B. 1992, *Information Protection and Other Unnatural Acts - Every Manager's Guide to Keeping Vital Computer Data Safe and Sound*, AMACOM, New York

Denning, P.J., 1990, "Computers Under Attack: Intruders, Worms, and Viruses", ACM Press, Addison-Wesley Publishing Company, Reading, Massachusetts, USA

Denzin, N.K. & Lincoln, Y.S. 1994, 'Introduction: Entering the Field of Qualitative Research', in Denzin & Lincoln (Eds) Handbook of Qualitative Research, Sage, Thousand Oaks, USA

Devargas, M., 1993, '*Network Security*', NCC Blackwell, Oxford, UK

Dexter A, Janson M, Kiudorf E, Laast-Laas J. 1993, 'Key Information Technology Issues in Estonia', *The Journal of Strategic Information Systems*, June, 2(2), pp 139-152

Dhillon G. & Backhouse J. 1994a, 'Responsibility Analysis: A Basis for Understanding Complex Managerial Situations', *The 1994 International Systems Dynamics Conference,* University of Stirling, Scotland, July

Dhillon G. & Backhouse J. 1994b, 'The Use of Information Technology in Organisations: Dealing with Systemic Opportunities and Risks', *Proceedings of the Second SISnet Conference*, Barcelona, September

Dhillon G. & Backhouse J. 1995, '*Computer Fraud: Its Management and Control*', CSRC/95/1, Computer Security Research Centre, London School of Economics and Political Science, London, UK

Dick, B. 1992, 'Qualitative Action Research: Improving the Rigour and Economy', *Second World Congress on Action Learning*, University of Queensland, Australia

Dick, B. 1993, '*You want to do an Action Research Thesis*?', Brisbane: Interchange (mimeo)

Dickson G., Leitheiser R., Wetherbe J. and Nechis M. 1984, "Key Information Systems Issues for the 80's", *MIS Quarterly*, Vol 8, No 3, September, pp 135-159

DOCIT, 1988, '*Information Technology Security Guidelines*', Department of Computing and Information Technology, Government of Western Australia

DOCIT, 1989, *'Disaster Recovery and Contingency Planning Manual'*, Department of Computing and Information Technology, Government of Western Australia

Drinan, J., 1991, 'Reflections of the First Day's Proceedings: Values and Action Research, in *Action Learning for Improved Performance*, Ed Zuber-Skerritt, AEBIS Publishing, Brisbane, Australia

Duncan, R.J., 1995, 'There are some Cracks in the Cornerstone of Information Security', *Computers & Security*, Vol. 14, No. 8, pp 675-680

Dutton, W.H., 1981, 'The Rejection of an Innovation: The Political Environment of a Computer-Based Model', *Systems, Objectives, Solutions*, vol. 1, no. 4, November, pp 179-201

Earl M. 1988, "*Information Management: The Strategic Direction*", Clarendon Press, Oxford

Edelson, L.W., & Parker, X.L., 1995, 'A Software Quality Assurance Methodology: SQA 2000', *IS Audit & Control Journal*, Vol 1, pp 42-44

Edwards, B., 1991, Safeguarding Corporate Data, Proceedings of EDPAC '91, Canberra, May, pp 149-158

Eisenhardt, K., 1989, 'Building Theories from Case Study Research', *Academy of Management Review*, vol. 14, no. 4, pp 532-550

Eisner, E.W., 1981, 'On the Differences Between Scientific and Artistic Approaches to Qualitative Research', *Educational Researcher,* vol. 10, no. 4, April, pp 5-9

Ekenberg L, Oberoi S. & Orci I., 1994, A Cost Model for Managing Information Security Hazards, *Proceedings of the Tenth International IFIP Conference on Computer Security*, IFIP SEC '94, May, Curacao

Elbra, R.A., 1992, '*Computer Security Handbook*', NCC Blackwell, Oxford, UK

Ellyard, D., 1993, *'Astronomy of the Southern Sky'*, Harper Collins Publishers, Australia

Engler N. 1995, 'Lax Security: Is It Negligence?', *Open Computing*, July, pp 45-49

Er M.C. 1986, "Classic Tools of Systems Analysis - Why They have Failed" *Data Processing*, Vol 11, pp 512-513

Ernst & Young, 1993, '*A Practical Approach to Logical Access Control*', McGraw-Hill International (UK) Limited

Ernst & Young, 1998, '*2nd Annual Global Information Security Survey*', E&Y Information Systems Assurance & Advisory Services, [www.ey.com/global/vault.nsf/US/2nd_Annual_Global_Information_Security_Survey/$file/FFO157.pdf]

European Security Form, 1995a, "Status Survey Underlines Need for More Action" *Forum*, Winter, p 3

European Security Forum, 1995b, "The Common Denominator" *Forum*, August, 2, p8

European Union, The Council, 1995, '*On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such data*', Brussels, June

Fagan, P., 1993, "Organisational Issues in IT Security', *Computers & Security*, vol. 12, no. 8, December, pp 710-715

Farrell, R., 1987, 'A Guide to Software Quality for the Developer and Unwary User', *The Australian Computer Journal*, Vol 19, No 4, November, pp 219-221

Farrow, R., 1991, 'UNIX System Security', Addison Wesley, Reading, Massachusetts, USA

Fillery, P.F., 1996, '*Pragmatic Quality Assurance in a Software Development, Installation and Maintenance Environment*', Masters Thesis, Curtin University of Technology, Perth, Western Australia

Fink, D., 1997, '*Information Technology Security*', CCH Australia

Firth D. 1993, 'Are We Securing the Right Information?', *Proceedings of the Tenth World Conference on Computer Security, Audit and Control*, COMPSEC '93, London, May, Elsevier Advanced Technology, pp 68-73

Fisher, R.P. 1984, *'Information Systems Security'*, Prentice-Hall, Englewood Cliffs, New Jersey

Fitzgerald, G., Hirschheim, R.A., Mumford, E., & Wood-Harper, A.T., 1985, 'Information Systems Research Methodology: An Introduction to the Debate', in Mumford, Hirschheim, Fitzgerald & Wood-Harper (Eds), '*Research Methods in Information Systems*', North-Holland, Netherlands, pp 3-12

Fitzgerald G., Stokes N. and Wood J. (1985) "Feature Analysis of Contemporary Information Systems Methodologies", *The Computer Journal*, Vol 28, No 3, pp 223-230

Fitzgerald, J., 1992, 'Twenty Safeguards for Data Communication Networks', *Information Management & Computer Security Journal*, vol. 10, no. 2, pp 4-7

Fitzgerald K. 1985, "Security of End-User Computing", *Computer Control Quarterly*, Winter, pp 19-20

Fitzgerald K. 1990, "The Security of Information - In an End-User Environment", *The Password*, February, pp 6-8

Fitzgerald, K. 1991, 'Computer Crime Detection', *Computer Control Quarterly*, vol. 9, no. 3, pp 41-48

Fitzgerald, K., 1992a, 'Network Security Issues', *Computer Control Quarterly* , vol. 10, no. 2, pp 16-20

Fitzgerald, K., 1992b, 'Privacy versus Fraud Control', *Computer Control Quarterly*, vol. 10, no. 2, pp 36-39

Fitzgerald, K., 1992c, 'Guidelines for Secure Computer Room Design', *Computer Control Quarterly*, vol.10, no.3, pp43-44

Fletcher, S. 1994, 'The Risk-Based Information System Design Paradigm', *Proceedings of the Tenth IFIP International Conference on Computer Security, IFIP SEC '94, Curacao*, May

Forbes, P. 1992, 'Conflicts Between the Drive for Efficiency and the Need to Define Effectiveness: Experiences in Action Research', *Proceedings of the Second World Congress on Action Learning*, July, Brisbane, pp 82-85

Forcht, K.A. 1994, '*Computer Security Management*', Boyd & Fraser Publishing Company, Massachusetts, USA

Forester, T. & Morrison, P. 1990, '*Computer Ethics*', Basil Blackwell, Oxford, UK

Fowler, J., 1996, 'Developing the Security Culture at the SEISMED Reference Centres', in Barber, Treacher & Louwerse, (Eds), "*Towards Security in Medical Telematics*", IOS Press, Amsterdam, pp 156-161

Frangos, S.A., 1996, 'Software Quality Assurance: the underlying Framework for Achieving Secure and Reliable Software Systems', in Katsikas, S. & Gritzalis, D. (Ed's), '*Information Systems Security*', Chapman and Hall, London, pp 465-474

Franz, C. & Robey, D. 1984, 'An Investigation of User-Led Systems Design: Rational and Political Perspectives', *Communications of the ACM*, vol. 27, no. 12, December, pp 1202-1217

Frenzel, C.W., 1992, "Management of Information Technology", Boyd & Fraser, Boston, Massachusetts, USA

Fulk, J, & Dutton, W., 1984, 'Videoconferencing as an Organisational Information System: Assessing the Role of Electronic Meetings', *Systems, Objectives, Solutions*, vol. 4, no. 2, April, pp 105-118

Furnell, S. and Sanders, P., 1996, 'The SEISMED Guidelines for Host Systems Security', in Barber, Treacher & Louwerse, (Eds), "*Towards Security in Medical Telematics*", IOS Press, Amsterdam, pp 150-155

Gable, G.G., 1994, 'Integrating Case Study and Survey Research Methods: an Example in Information Systems', *European Journal of Information Systems*, vol. 3, no. 2, pp 112-116

Galliers, R. 1987, 'Information Systems Planning in the United Kingdom and Australia: A Comparison of Current Practice' in Zorkorczy (Ed) "*Oxford Surveys in Information Technology*", vol. 4, pp 223-255

Galliers, R. 1991, 'Choosing Appropriate Information Systems Research Approaches: A Revised Taxonomy', in Nissen, Hirschheim & Klein (Eds) "*The Information Systems Research Arena of the 90's*" North-Holland

Galliers, R. Merali, Y. & Spearing, L. 1994, 'Coping with Information Technology? How British Executives Perceive the Key Information Systems Management Issues in the mid-1990s', *Journal of Information Technology*, vol. 9, no. 3

Galliers, R. & Land, F. 1987, 'Choosing Appropriate Information Systems Research Methodologies', *Communications of the ACM*, vol. 30, no. 11, November, pp 900-902

Galliers, R. and Land, F. 1988, 'The Importance of Laboratory Experimentation in IS Research', *Communications of the ACM*, vol. 31, no. 12, pp 1502-1505

Gardner, J. 1989, 'Computer Fraud - It Can't Happen to Us', *Computer Control Quarterly*, vol. 7, no. 3, p 46

Garfinkel, S. & Spafford, G., 1991, '*Practical UNIX Security*', O'Reilly & Associates Inc., Sebastopol, CA, USA

Garner R., 1995, 'The Growing Professional Menace', *Open Computing*, July, pp 33-42

Gartner Group 1997, 'Technology's Top 10 Trends', *MIS Magazine*, October Supplement, pp7-15

Gasser M., 1988, *Building a Secure Computer System*, Van Nostrand Reinhold, New York, USA

Gaunt, N. and Roger-France, F., 1996, 'Security of the Electronic Health Care Record – Professional and Ethical Implications', in Barber, Treacher & Louwerse, (Eds), "*Towards Security in Medical Telematics*", IOS Press, Amsterdam, pp 10-22

Gerrity T.P. and Rockart J.F., 1986, "End-User Computing: Are you a Leader or a Laggard?", *Sloan Management Review*, Summer, pp 25-34

Gersick, C., 1988, 'Time and Transition in Work Teams: Toward a New Model of Group Development', *Academy of Management Journal*, vol. 31, pp 9-41

Gibson, C.F. and Nolan, R.L., 1974, 'Managing the Four Stages of EDP Growth', Harvard Business Review, January-February

Grant, C., 1991, Computer Security Improvement via Risk Analysis, *Proceedings of EDPAC '91*, Canberra, May, pp197-202

Grosvenor, G.M., Allen, W.L. & Shupe, J.F., 1995, 'Star Birth in the Orion Nebula', National Geographic, vol. 188, no. 6, December, Supplement

Gummesson, E. 1991, 'Qualitative Methods in Management Research', Sage, Newbury Park

Hafner, K. and Markoff, J., 1993, "Cyberpunk: Outlaws and Hackers on the Computer Frontier", Corgi Books, Great Britain

Hains, D., 1992a, 'A Security Questionnaire for IT Adults Only', *Computer Control Quarterly*, vol.10, no.3, pp 38-42

Hains, D., 1992b, 'LAN Security: Are you taking it Seriously?', *Computer Control Quarterly*, vol.10, no.1, pp 7-11

Hamilton, S. & Ives, B. 1982, 'MIS Research Strategies', *Information & Management,* vol. 5, pp 339-347

Hancock, B., 1998, 'Network Breaches: They are Real', *Computer Fraud & Security,* October, pp 8-11

Hancock, B., 1999, 'Security Views', *Computers & Security*, vol. 18, pp 184-198

Harker, M., 1991, 'The Legitimisation of Action Research and Action Learning for Management – When Will it Happen?', in Colins, C. and Chippendale, P. (Ed's), 'Action Research and Process Management', Acorn Publications, Queensland, pp 109-118

Harmon, C., 1998, 'Safeguarding the Data Warehouse', *Computer Fraud & Security*, June, pp 16-19

Harre, R. 1972, ' *The Philosophies of Science*, An Introductory Survey', Oxford University Press, London

Harris M. 1988, "Controlling User Driven Development" *The Password*, April, pp 1-6

Harris, S., & Sutton, R., 1986, 'Functions of Parting Ceremonies in Dying Organisations', *Academy of Management Journal*, vol. 29, pp 5-30

Harrison W, and Farn C. 1990, 'A Comparison of Information Management Issues in the United States of America and the Republic of China', *Information & Management*, April, 18(4), pp 177-188

Hartley R J, 1993, 'Fraud Management: Assessment, Prevention, Control', *Proceedings of the Fourth Pacific Region Security Conference*, 1-3 June, Melbourne

Hartog, C. & Herbert, M. 1986, '1985 Opinion Survey of MIS Managers: Key Issues', *MIS Quarterly*, December, pp 350-361

Henderson, S. 1995, 'The Quandary of Rigour in Qualitative Research', in proceedings of conference "Qualitative Research: Beyond the Boundaries", Fremantle, Western Australia, 21-22 November

Henry, C., 1991, 'Reflections at the End of the Congress: If Action Research were Tennis', in *Action Learning for Improved Performance*, Ed Zuber-Skerritt, AEBIS Publishing, Brisbane, Australia, pp 102-115

Herbert, M. & Hartog, C. 1986, 'MIS Rates the Issues', *Datamation*, November, pp 79-86

Hirschheim R. 1983, "Assessing Participative Systems Design: Some Conclusions from an Exploratory Study" *Information & Management*, Vol 6, pp 317-327

Hirschheim R. 1985, "User Experience with and Assessment of Participative Systems Design" *MIS Quarterly*, vol. 9, no. 4, December, pp 295-304

Hirschheim R. 1986, "Participative Systems Design: User Experiences Evaluation and Conclusions", *Australian Computer Journal*, Vol 18, No 4, November, pp 166-173

Hirschheim, R., Klein, H. & Lyytinen, K., 1995, '*Information Systems Development and Data Modelling: Conceptual and Philosophical Foundations*', Cambridge University Press, Cambridge, UK

Hitchings J. 1994, 'The Need for a New Approach to Information Security', *Proceedings of IFIP SEC 94*, Curacao, May

Hitchings, J. 1995, 'Achieving an Integrated Design: The Way Forward for Information Security', in Eloff J.H.P. & von Solms S.H. (Ed's), '*Information*

Security - the Next Decade', Proceedings of the IFIP TC11 eleventh international conference on information security, Johannesburg, May, Chapman & Hall, pp 369-383

Hitchings, J,. 1996, 'A practical solution to the complex human issues of information security design', in Katsikas, S. & Gritzalis, D. (Ed's), '*Information Systems Security'*, Chapman and Hall, London, pp 3-12

Hoath, P. & Mulhall, T., 1998, 'Hacking: Motivation and Deterrence, Part 1', *Computer Fraud & Security*, April, pp 16-18

Hoffer, J. & Straub, D., 1989, 'The 9 to 5 Underground: Are You Policing Computer Crimes?', *Sloan Management Review*, Summer, p 38

Holbein, R., Teufel, S., Morger, O. and Bauknecht, K., 1997, 'A Comprehensive Need-to-Know Access Control System and its Application for Medical Information Systems', in Yngstrom, L. and Carlsen, J. (Ed's), "Information Security in Research and Business", Chapman and Hall, London, pp 78-90

Hopkinson, P., 1992a, 'The Importance of Security Standards, *Computer Control Quarterly,* vol. 10, no. 3, pp 33-37

Hopkinson, P., 1992b, 'Contingency Planning in the Distributed Environment', *Computer Control Quarterly,* vol. 10, no. 1, pp 27-29

Hopkinson, P., 1992c, 'Fraud Limitation: A Practical Approach', *Computer Control Quarterly,* vol. 10, no. 4, pp 22-26

Hoppe, N., 1994, 'Achieving Consistent Security Controls Throughout a Multinational Organisation', *Computers & Security*, vol. 13, no. 1, February, pp 23-29

Howard, G., 1988, 'Toward a General Taxonomy of MIS Research: A Progress Report on Defining the Discipline', *The Journal of Computer Information Systems*, Fall, pp 9-14

Hough, N., 1991, Digital Signatures and Data Encryption - The Ultimate Safeguards!, Proceedings of EDPAC '91, Canberra, May, pp 245-264

Hughes, L.J., 1995, '*Internet Security Techniques'*, New Riders, Indiana

Hult, M., & Lennung, S.A., 1980, 'Towards a Definition of Action Research: A Note and Bibliography', *Journal of Management Studies*, vol. 17, no. 2, pp 241-250

Humphreys, T., 1996, 'Security Standards for Medical Information Systems', in Barber, Treacher & Louwerse, (Eds), "*Towards Security in Medical Telematics*", IOS Press, Amsterdam, pp 131-144

Hussain, D. & Hussain K.M. 1988, 'Managing Computer Resources', Irwin, Illinois, 2nd Edition

Icove, D., Seger, K. & VonStorch, W., 1995, *'Computer Crime: A Crimefighter's Handbook'*, O'Reilly & Associates, CA, USA

ISACA, 1995, *COBIT Framework: Control Objectives for Information and Related Technology*, Information Systems Audit and Control Association, Illinois, USA

ISACF, 1995, *'CobiT: Control Objectives for Information and Related Technology, Executive Summary'*, Information Systems Audit and Control Foundation, Illinois, USA

Ives, B. & Olson, M., 1981, 'Manager or Technician? The Nature of the Information Systems Manager's Job', *MIS Quarterly*, vol. 5, no. 4, December, pp 49-63

Ives, B. & Olson, M., 1984, 'User Involvement and MIS Success: A Review of Research', *Management Science*, vol. 30, no. 5, May, pp 586-602

Jackson B. 1986, 'Information Security and Privacy', *EDP Analyzer*, February, vol. 24, no.2

Jackson, K.M. and Hruska, J. (Ed's) 1992, *'Computer Security Reference Book'*, Butterworth Heinemann, Oxford UK

Jackson, P., 1992, 'Backup for Personal Computers', in Jackson, K.M. & Hruska, J., 1992, *'Computer Security Reference Book'*, Butterworth Heinmann, Oxford, UK, pp 617-639

Jaehne, E.M. 1984, 'Security and Productivity', *in Computer Security: A Global Challenge*, eds Finch and Dougall, Elsevier Science Publishers, North-Holland

James, H.L., 1994a, *'The Exploitation of Computers: An Analysis of Computer Abuse Cases'*, Working Paper, School of IS, Curtin University of Technology, Perth WA

James, H.L., 1994b, 'Open versus Closed Systems Security', Proceedings of the Second Computer Security Conference, Singapore Institute of Management, Singapore, July 20-22

James, H.L., Andronis, K. and Paul, W., 1996, 'A Human Approach to Security Management in HealthCare', in Katsikas, S. and Gritzalis, D. (Ed's), "*Information Systems Security*", Chapman and Hall, London, pp 365-376

James, H.L. and Chantler, A.N., 1993a, *'Managing Computer Security'*, IS Publishers, Curtin University of Technology, Perth Western Australia

James, H.L. and Chantler, A.N., 1993b, 'Logical Access Security in Open Systems Networks', in Vogel, Glasson, Marshall & Verrijn-Stuart (Eds), *'Local Area Network Applications: Leveraging the LAN'*, North-Holland IFIP, Netherlands, pp 261-262

James, H.L. and Chantler, A.N., 1993c, *'Network Access: Risks and Security Measures'*, Working Paper No. 93.01, Curtin University of Technology, Perth Western Australia

James, H.L. and Chantler, A.N., 1994, 'Computer Hackers - Ingenious Programmers or Cyberpunks?', *Proceedings of EDPAC '94* , May 16-18, Gold Coast, Queensland, Australia

James, H. and Coldwell R.A., 1993, 'Corporate Security: An Australian Ostrich', *Information Management & Computer Security*, vol. 1, no. 4, pp 10-12

James H. and Morien R. 1991, "Controlling Rapid Information Systems Development Environments", *Proceedings of EDPAC 91*, Canberra, May, pp 287-305

Janson, M. and Smith, L. 1985, 'Prototyping for Systems Development: A Critical Appraisal', *MIS Quarterly*, June, pp 141-156

Jarvenpaa, S.L., Dickson, G.W. and DeSanctis, G., 1985, 'Methodological Issues in Experimental IS Research: Experiences and Recommendations', *MIS Quarterly*, June, pp 141-156

Jensen, E., 1994, 'Firewalls a must for Internet Security', *Computerworld*, September 23, p14

Jick, T.D., 1979, 'Mixing Qualitative and Quantitative Methods: Triangulation in Action', *Administrative Science Quarterly*, vol. 24, pp 602-611

Jick, T.D., 1983, 'Mixing Qualitative and Quantitative Methods: Triangulation in Action', in J. Van Maanen (Ed) '*Qualitative Methodology*, Sage Publications, Beverly Hills, CA, USA, pp 135-148

Jones, J., 1991a, 'Making Metaphors: Breaking Frames', in *Action Research & Process Management*, eds Colins & Chippendale, Acorn Publications, Queensland, Australia, pp 159-168

Jones, J., 1991b, 'Reflections on the Second Day's Proceedings: Gazing into Muddy Waters', in *Action Learning for Improved Performance*, Ed Zuber-Skerritt, AEBIS Publishing, Brisbane, Australia

Kamay, V. & Adams, T., 1990, 'The 1990 Profile of Computer Abuse in Australia', *Computer Control Quarterly*, vol. 8, no. 4, pp 12-27

Kamay, V. & Adams, T., 1992, *'The 1992 ACARB Profile of Computer Abuse in Australia'*, ACARB at RMIT, Melbourne

Kanter, J. 1986, 'The Role of Senior Management in MIS', *Journal of Systems Management*, April, pp 10-17

Kaplan, B. & Duchon, D. 1988, 'Combining Qualitative and Quantitative Methods in Information Systems Research: A Case Study', *MIS Quarterly*, December, pp 570-586

Katsikas, S., 1996, 'The SEISMED High Level Security Policy for Health Care', in Barber, Treacher & Louwerse, (Eds), "*Towards Security in Medical Telematics*", IOS Press, Amsterdam, pp 125-130

Keen P. 1984, "Building the Information Systems Research Community" *Information Technology Training*, November, pp 129-132

Keen P.G. 1988a, "*Competing in Time*", Ballinger, USA

Keen P.G. 1988b, "Rebuilding the Human Resources of Information Systems" in Earl, "*Information Management the Strategic Dimension*", Oxford Clarendon Press, Oxford

Keen, P., Bronsema, G. & Zuboff, S., 1982, 'Implementing Common Systems: One Organisation's Experience', *Systems, Objectives, Solutions*, vol. 2, no. 3, August, pp 125-142

Kemmis, S. and McTaggart, R. 1988, '*The Action Research Planner*', 3rd Ed, Deakin University Press, Geelong, Australia

Kennedy, S. 1994, 'Why Users Hate Your Attitude', *Informatics*, February, pp 29-32

Khandeker J. and Langer M. 1990, "Personal Computers: An Audit Perspective" *Internal Auditor*, October, pp 55-61

Kiountouzis E. & Kokolakis S. 1996, An Analyst's View of IS Security, , in Katsikas, S. and Gritzalis, D. (Ed's), "*Information Systems Security*", Chapman and Hall, London, pp 23-35

King W.R., 1994, Strategic Planning for Management Information Systems, in Gray P, King W, McLean E & Watson H. (Eds) *Management of Information Systems,* Dryden Press, Fort Worth, Texas, USA, pp 334-348

Kleeman, D., 1991, A Risk based Approach to Designing Controls into Computer Systems', Proceedings of EDPAC '91, Canberra, May, pp 313-322

Klein, G., 1996, 'Trusted Health Information Systems: A Project within the DG XIII/INFOSEC Programme on Electronic Signatures and Trusted Third Parties', in Barber, Treacher & Louwerse, (Eds), "*Towards Security in Medical Telematics*", IOS Press, Amsterdam, pp 238-245

Klosky, M., Gallegos, F. & Klosky, V., 1995, 'Information Protection and Security: A Perspective', *IS Audit & Control Journal*, vol.V, pp 6-11

Kogan, A., Sudit, E.F. & Vasarhelyi, M.A., 1996, 'Internet: A Technical Primer', *IS Audit & Control Journal,* vol.I, pp 24-27

Koory J. and Medley D. 1987, *"Management Information Systems: Planning and Decision Making*" South-Western, California

Kowalski, S., 1991a, 'A SBC Modelling of USA's National Computer Security Policy', *Computers & Security*, Vol 10, No. 3

Kowalski, S., 1991b, 'The SBC Model: Modelling the System for Consensus', *Proceedings of the 7th IFIP TC11 Conference on Information Security*, Brighton, UK, May

Kowalski, S., 1993, 'Reporting IT Crimes: SBC as a Conceptual Framework', *Proceedings of IFIP WG 9.6 Conference*, Petersburg, August

Kowalski, S., 1994, '*IT Insecurity: A Multi-Disciplinary Inquiry*', Report Series No. 94-004, Department of Computer and Systems Sciences, Stockholm University, Sweden

KPMG, 1993, '*Fraud Awareness Survey*', KPMG Peat Marwick, March, Sydney, Australia

KPMG, 1996, '*International Fraud Report*', KPMG International Headquarters, Netherlands, [http://www.kpmg.net/images/library/96/may/fraud.pdf]

KPMG, 1997, '1997 KPMG Canadian Fraud Survey Report', KPMG Canada, [http://www.kpmg.ca/isi/vl/frsur97e.htm]

KPMG, 1998, '*Information Security Survey 1998*', KPMG UK, [http://www.kpmg.co.uk/uk/services/irm/iss98/index.html]

KPMG, 1999a, '*1999 KPMG Fraud Survey*', KPGM Australia, [http://www.kpmg.com.au/fraud1.html]

KPMG, 1999b, '1999 KPMG Canadian Fraud Survey Report', KPMG Canada, [http://www.kpmg.ca/isi/vl/frsur99e.htm]

Krueger, K.H., 1993, 'Internal Control by Objectives: The Functional Control Matrix', in Dougall E.G. & Jones, D (Ed's), '*Computer Security: Discovering Tomorrow*', Proceedings of the Ninth IFIP International Symposium on Computer Security, Ontario, Canada, May 12-14, pp 151-164

Kruger, R. and Eloff, J., 1997, 'A Common Criteria Framework for the Evaluation of Information Technology Systems Security', in Yngstrom and Carlsen (Eds),

"*Information Security in Research and Business*", Chapman and Hall, London, pp 197-209

Krull A., 1986, "Management Controls for Personal Computers: An Internal Auditor's Overview", *Computer Control Quarterly*, Winter, pp 35-40

Krupp, E.C., 1996, 'The Thread of Time', *Sky and Telescope*, January, pp 60-61

Kuhn, T., 1970, '*The Structure of Scientific Revolutions*', 2nd Edition, University of Chicago Press, Chicago, USA

Kurzban, S.A., 1986, 'Computing Systems Defences', *SIG Security Audit & Control Review, ACM,* vol.4, no.1, pp 1-27

Kwok, L., and Longley, D., 1997, A Standard for Information Security Management, in Yngstrom, L., and Carlsen, J. (Ed's), "*Information Security in Research and Business*", Chapman and Hall. London, pp 78-90

Labuschagne, L. & Eloff, J.H.P., 1996, Activating Dynamic Counter Measures to Reduce Risk, in 'Information Systems Security', in Katsikas S.K. & Gritzalis D. (eds), "*Information Systems Security*", Chapman & Hall, London, pp 187-196

Lafleur, L.M., 1992, 'Training as Part of a Security Awareness Programme', *Information Management & Computer Security Journal*, vol. 10, no. 4, pp 4-11

Land F. 1982, "Adapting to Changing User Requirements", *Information & Management*, Vol 5, pp 59-75

Landreth, B., 1989, '*Out of the Inner Circle*', Tempus Books, Washington, USA

Lane V.P. 1985, *Security of Computer Based Information Systems*, MacMillan

Laske, C., 1996, 'Legal Issues in Medical Informatics: A Bird's Eye View', in Barber, Treacher & Louwerse, (Eds), "*Towards Security in Medical Telematics*", IOS Press, Amsterdam, pp 53-78

Ledington, J. & Ledington, P., 1999, 'Decision-Variable Partitioning: an Alternative Modelling Approach in Soft Systems Methodology', *European Journal of Information Systems*, vol. 8, pp 55-64

Lee, A., 1989, 'A Scientific Methodology for MIS Case Studies', *MIS Quarterly*, March, pp 32-50

Levenson, N. and Turner, C., 1993, 'An Investigation of the Therac-25 Accidents', *IEEE Computer*, July, pp 18-41

Leveson, N.G., 1995, "*Safeware: System Safety and Computers*", Addison-Wesley, Reading, Massachusetts, USA

Lindup, K.R., 1995, 'A new model for information security policies', *Computers & Security*, Vol. 14, No. 8, pp 691-695

"Listen: Computer Crime Victims Speak", *Datamation*, December 15, 1995, p 20

Louwerse, K., 1996, 'How to Assure Security: CEN Standards, Directives or European Guidelines?', in Barber, Treacher & Louwerse, (Eds), *"Towards Security in Medical Telematics"*, IOS Press, Amsterdam, pp 145-149

Lowe, I., 1991, 'Epilogue: Action Research for a Better World', in *Action Learning for Improved Performance*, Ed Zuber-Skerritt, AEBIS Publishing, Brisbane, Australia

Lubelski, J. & Kocher, P., 1995, 'Automated Testing: The Promises and Pitfalls', *IS Audit & Control Journal*, vol.I, pp 46-48

Lyytinen K., 1987, "Different Perspectives on Information Systems: Problems and Solutions", *ACM Computing Surveys*, Vol 19, No 1, March, pp 5-46

MacQuarie Encyclopedic Dictionary, 1990, The MacQuarie Library, MacQuarie University, NSW, Australia

Madron, T.W., 1992, *'Network Security in the 90's: Issues and Solutions for Managers'*, Wiley, New York

Mahmood M. and Becker J., 1985, "Effect of Organisational Maturity on End-Users Satisfaction with Information Systems" *Journal of Management Information Systems*, Vol 2, No 3 pp 37-64

Main, A., 1995, 'Sec, Lies and Policy Manuals', *Proceedings of the Fifth Annual AUUG Conference*, February, Perth, Western Australia

Malin, D. & Frew, D.J., 1995, *'Hartung's Astronomical Objects for Southern Telescopes'*, Melbourne University Press

Marcus M. and Robey D., 1988, "Information Technology and Organisational Change: Causal Structure in Theory and Research", *Management Science*, Vol 34, No 5, May, pp 583-598

Markey E., 1989, "Getting Organizations involved in Computer Security: The Role of Security Awareness", in Caelli W.J. (Ed), (1989), "Computer Security in the Age of Information", Elseveir Science Publishers B.V. (North Holland), IFIP, pp 83-86

Markoff J., 1993, Computer Insecurity on the Rise, *New York Times*, November 1, p D1

Marro P.E., 1995, Overview of Computer Crime and Security, *IS Audit & Control Journal*, Vol V, pp 20-25

Martin, D., 1992, 'Software Methods', in Jackson, K.M. & Hruska, J., 1992, *'Computer Security Reference Book'*, Butterworth Heinmann, Oxford, UK, pp 291-310

Martin, J., 1973, *'Security Accuracy and Privacy in Computer Systems'*, Prentice-Hall, Englewood Cliffs, New Jersey

Maxwell, J.A., Bashook, P.G., & Sandlow, L.J., 1986, 'Combining Ethnographic and Experimental Methods in Educational Research: A Case Study', in D.M. Fetterman and M.A. Pitman (eds), *'Education Evaluation: Ethnographic in Theory, Practice, and Politics'*, Sage Publications, Beverly Hills, CA, USA, pp 121-143

McCouat, M. & Peile, C., 1995, "The Micro Politics of Qualitative Research Traditions", Conference Proceedings, *'Qualitative Research: Beyond the Boundaries'*, Fremantle, Western Australia, November 21-22

McCoy, P. 1994, 'Removing the Bloody Axe', *Informatics*, February, p 34

McCumber, J., 1991, 'Information Systems Security: a Comprehensive Model', *Proceedings of the 14th National Computer Security Conference*, NCSC, October, pp 329-337

McCusker T,. 1994, 'Take Control of Remote Access', *Datamation*, April 1, pp 62-64

McNurlin B.C. and Sprague R.H., 1989, *"Information Systems Management in Practice"* Second Edition, Prentice-Hall, USA

McKernan, J., 1991, 'Some Developments in the Methodology of Action Research: Studied Enactment', in Colins, C. and Chippendale, P. (Ed's), *'Action Research & Process Management'*, Acorn Publications, Queensland, Australia, pp 43-56

McKernan, J., 1992, 'Action Research as the Basis for Teaching, Learning and Professional Development', *in Proceedings of the Second World Congress on Action Learning*, July, Brisbane, pp 32-46

Menkus B. 1991, 'Control is Fundamental to Successful Information Security', *Computers & Security*, 10, pp 293-297

Metchik, E., 1997, 'A Typology of Crime on the Internet', *Security Journal*, vol. 9, pp 27-31

Middleton, P.E. 1992, 'Foreword', *Proceedings of the Inaugural Series of Lectures in Business Ethics*, Curtin Business School, Curtin University of Technology, Perth, Western Australia, p iv

Miles, M.B. & Huberman, A.M., 1984, 'Drawing Valid Meaning from Qualitative Data: Toward a Shared Craft', *Educational Research*, vol. 13, no. 5, pp 20-29

Mintzberg, H., & McHugh, A., 1985, 'Strategy Formation in an Adhocracy', *Administrative Science Quarterly*, vol. 30, pp 160-197

Moeller, R., 1989, '*Computer Audit, Control and Security*', John Wiley & Sons, New York

Moignard, P., 1995, 'Trends in Systems Development', *IS Audit & Control Journal*', vol.I, pp 10-13

Moore R.H., 1994, Wiseguys: Smarter Criminals and Smarter Crime in the 21st Century, *Futurist*, 28(5), pp 33-37

Morgan, G. & Smircich, L., 1980, 'The Case for Qualitative Research', *Academy of Management Review*, vol. 5, no. 4, pp 491-500

Mostert D. & von Solms S., 1993, Integrating Computer Security, Safety and Resilience into User Requirements, *Proceedings of the Tenth World Conference on Computer Security, Audit and Control, COMPSEC '93*, London, May, Elsevier Advanced Technology, pp 141-157

Mumford E. 1981, "Participative Systems Design: Structure and Method" *Systems, Objectives, Solutions*, Vol 1, No 1, pp 5-19

Mumford E. 1983, "*Designing Human Systems*", Manchester Business School, Manchester, England,

Mumford E. 1985, "Defining Systems Requirements to Meet Business Needs: A Case Study Example", *Computer Journal*, Vol 28, No 2, pp 97-104

Mumford E., Land F. and Hawgood J. 1978, "A Participative Approach to the Design of Computer Systems" *Impact of Science on Society*, Vol 28, No 3, pp 235-253

NCC, 1994, "*IT Security Breaches Survey Summary*", National Computing Centre Limited, UK

Nelson, R., 1997, 'The Future of Networks and Network Security', in Yngstrom, L., and Carlsen, J. (Ed's), '*Information Security in Research and Business*', Chapman and Hall. London, pp 417-424

Neumann, P.G., 1995, '*Computer Related Risks*', Addison-Wesley Publishing Company, Reading, Massachusetts, USA

New Hamlyn, 1988, '*Encyclopedic World Dictionary*', Golden Press, London

Newman, T., 1993, 'Information Loss Rarely Recovered', *Information Management & Computer Security Journal,* vol. 1, no. 4, pp 17-18

Niederman F, Brancheau J, Wetherbe J, 1991, Information Systems Management Issues for the 1990s, *MIS Quarterly*, December, 17(4), pp 475-500

NRC, 1991, '*Computers at Risk: Safe Computing in the Information Age*', System Security Study Committee Computer Science and Telecommunications Board Commission on Physical Sciences, Mathematics, and Applications, National Research Council, National Academy Press

OAG, Office of the Auditor General, 1992, '*Management of Information Systems in the Public Sector*', Report of the Auditor General to the Western Australian Parliament

O'Donoghue J. 1987, "Strategies Found to be Effective in the Control of Computer Crime in the Forbes 500 Corporations", *Security Audit & Control Review*, Vol 5, No 1, Winter

OECD, 1992, ' *Guidelines for the Security of Information System's*, Organisation for Economic Cooperation and Development, OECD/GD(92)190, Paris

Olson M. 1981, "User Involvement and Decentralisation of the Development Function: A Comparison of Two Case Studies", *Systems Objectives Solutions*, Vol 1, No 2, April, pp 59-69

Olson M. and Ives B. 1981, "User Involvement in Systems Design: An Empirical Test of Alternative Approaches", *Information & Management*, Vol 4, No 4, pp 183-195

Orlandi E., 1986, "Nolan's Stage Model and Computer Security", in *Proceedings of the 1986 International Carnahan Conference on Security Technology*, Gothenburg, Sweden, August 12-14, pp 45-50

Otway, J., 1992, 'The Information Technology Security Project Plan', *Information Management & Computer Security Journal*, vol. 10, no. 4, pp 12-17

Page, D., Williams, P. & Boyd, D., 1993, *'Report of the Inquiry into the London Ambulance Service*', London: South West Thames Regional Health Authority

Paliotta, A.R., 1995, 'Protecting the Electronic Environment in the "New Technological World Order"', *IS Audit & Control Journal*, vol.VI, pp7-9

Palvia, P.C. & Palvia, S., 1992, MIS Issues in India and a Comparison with the United States, *International Information Systems*, pp 101-110

Pangalos, G. and Khair, M., 1996, 'Design of Secure Medical Database Systems', in Katsikas, S. and Gritzalis, D. (Ed's), "*Information Systems Security*", Chapman and Hall, London, pp 386-401

Parker, D.B., 1981, '*Computer Security Management*', Reston Publishing Company, Virginia, USA

Parker, D.B,. 1983, *'Fighting Computer Crime'*, Charles Scribner's Sons, New York

Parker, D.B., 1991, 'Restating the Foundation of Information Security', *Proceedings of the Seventh Asia Pacific Information Systems Control Conference*, Seoul Korea, October 14-18

Parker, D.B., 1998, *'Fighting Cyber Crime: A New Framework for Protecting Information'*, John Wiley & Sons, New York

Parker M, Benson R. and Trainor E., 1988, *'Information Economics: Linking Performance to Information Technology'*, Prentice-Hall, Englewood Cliffs, New Jersey

Parker, S., 1996, 'Images', *Sky and Telescope*, March, pp 20-21

Parkin, R., 1993, 'Directors Briefing Computer Security - An Implementation Strategy', *Proceedings of the Tenth World Conference on Computer Security, Audit and Control, COMPSEC '93, London*, May, Elsevier Advanced Technology, pp 369-381

Parkinson, M.J. & Paul, R. 1989, *'PC Taming: The Audit and Control of Microcomputers'*, EDP Auditors Association, Canberra, Australia, 2nd Edition

Passfield, R., 1991, 'Action Research: A Strategic HRM Process for Achieving Postmerger Integration?', in *Action Research & Process Management*, eds Colins & Chippendale, Acorn Publications, Queensland, Australia, pp 57-66

Patching, D., 1990, *'Practical Soft Systems Analysis'*, Pitman, London

Patel, A. and Kantzavelou, I., 1996, 'Issues of Security and Network Security in Health Care Information Systems', in Barber, Treacher & Louwerse, (Eds), "*Towards Security in Medical Telematics*", IOS Press, Amsterdam, pp 216-223

Pearson, P., 1992, 'Personal Computers', in Jackson, K.M. & Hruska, J., 1992, *'Computer Security Reference Book'*, Butterworth Heinmann, Oxford, UK, pp 565-592

Peile, C., 1994, *'The Creative Paradigm'*, Aldershot, USA

Peltier, T., 1998, 'How to Create a Data Classification Program', *Computer Security Journal*, vol. XIV, no. 2, pp 15-24

Perry, C. & Zuber-Skerritt, O., 1991, 'Action Research in Graduate Management Research Programs', in Colins C.J. & Chippendale P.J. (eds) *Proceedings of the First World Congress on Action Research & Process Management, Volume 1: Theory & Praxis Frameworks, Acorn Publications*, Queensland, Australia, pp 67-81

Pervan G.P., 1993, 'Results from a Study of Key Issues in Australian IS Management', *4th Australian Conference on Information Systems*, September, Brisbane, Queensland

Pfleeger C.P., 1997, '*Security in Computing*', Prentice-Hall, Englewood Cliffs, New Jersey, Second Edition

Porter M.E., 1980, "*Competitive Strategy*", The Free Press, New York

Power K., 1994, 'Crooks Among Colleagues', *Informatics*, November, pp 22-26

Power R., 1998, '1998 CSI/FBI Computer Crime and Security Survey', *Computer Security Journal*, vol. Xiv, no. 3, pp 31-42

Power R., 1999, '1999 CSI/FBI Computer Crime and Security Survey', *Computer Security Journal*, vol. Xv, no. 2, pp 29-43

Principal Financial Group, 1999, 'Information Security Program of the Year: Sample Policies and Procedures', *Computer Security Journal*, vol. XV, no. 1, pp 47-52

Purser, M., 1993, '*Secure Data Networking*', Artech House, MA, USA

Pyburn, P.J., 1983, 'Linking the MIS Plan with Corporate Strategy: An Exploratory Study', *MIS Quarterly*, vol. 7, no. 2, June, pp 1-14

Raab, C. & Williams, G., 1999, 'Privacy in the GII: Issues, Processes and Solutions', in Fischer-Hubner, Quirchmayr & Yngstrom, Eds, '*User Identification & Privacy Protection*', Proceedings of the Joint IFIP WG8.5 and WG9.6 Working Conference, Stockholm University, Sweden, pp 21-42

Randolph W. and Posner B. 1988, "*Effective Project Planning and Management*" Prentice-Hall, Englewood Cliffs, New Jersey

Reston, J., 1995, 'Orion: Where Stars are Born', *National Geographic*, vol. 188, no. 6, pp 88-101

Rhee, M.Y., 1994, '*Cryptography and Secure Communications*', McGraw-Hill Book Co., Singapore

Rindfleisch, T.C., 1997, "Privacy, Information Technology, and Health Care", Communications of the ACM, Vol. 40, No. 8, pp 93-100

Rodwell, M.K., 1990, 'Person / Environment Construct: Positivist Versus Naturalistic, Dilemma or Opportunity for Health Social Work Research and Practice', *Social Science and Medicine,* vol. 31, no. 1, pp 27-34

Roger-France, F. and Santucci, G., 1991, 'Perspectives of Information Processing in Medical Applications: Strategic Issues, Requirements and Options for the European Community', Springer Verlag, Berlin

Rothfeder J, 1993, ' Holes in the Net', *Corporate Computing*, May pp 114-120

Rushkoff, D., 1994, 'Cyberia', Flamingo Harper Collins Publishers, London, UK

Russell, S., 1994, 'Audit-by-Receiver Paradigms for Verification of Authorisation at Source of Electronic Documents', *Computers & Security*, vol. 13, no. 1, pp 59-67

Ryan H. 1990, "The Management Cycle: The Key to Control" *Journal of Information Systems Management*, Spring, pp 62-65

Saddingham, T. (1988) *'Security for Small Computer Systems'*, Elsevier Science, Oxford, UK

Sandelowski, M. (1986) 'The Problem of Rigour in Qualitative Research', Advances in Nursing Science, vol. 8, no. 3, pp 27-37

Sapienza, R.J., 1995a, 'Is Your Systems Development Train Falling Off its Tracks?', *IS Audit & Control Journal*, Vol 1, p 8

Sapienza, R.J., 1995b, 'Looking for the 800 lb Gorilla: An Interview with Bill Smillie', *IS Audit & Control Journal*, Vol 1, pp 15-18

Sawicki, E., 1992, *'LAN Desktop Guide to Security'*, SAMS-Prentice-Hall, Indiana

Schwartau, W., 1996, 'Creating Boundaries: Protecting Companies and Employees on the Information Superhighway', *IS Audit & Control Journal,* vol.I, pp 28-32

Seah V, Kamay V, Adams T, and Sung H, 1991, *A Study of Computer Security and Computer Abuse in Singapore - 1990,* SIM Monograph No. 3, Singapore Institute of Management

"Security", 1995, *Information Week*, November 27, pp 32-40

Senge, P.M., *'The Fifth Discipline – The Art & Practice of The Learning Organisation'*, Random House, Australia

Shaw, R., 1996, 'Safety and Security of Information Systems', in Barber, Treacher & Louwerse, (Eds), "*Towards Security in Medical Telematics*", IOS Press, Amsterdam, pp 190-199

Shepperd M. 1990, "Early Life-Cycle Metrics and Software Quality Models", *Information and Software Technology*, Vol 32, No 4, May/June, pp 311-316

Sherizan S. 1995, 'The Globalization of Computer Crime and Information Security', *Computer Security Journal*, Vol VIII, No 2, pp 13-19

Silverman, D., 1998, 'Qualitative Research: Meanings or Practices?', *Information Systems Journal,* vol. 8, no. 1, January, pp 3-20

Siponen, M. & Kajava, J., 1998, 'The Dimensions and Categories of Information Security Awareness', *Proceedings of the 1998 IFIP World Congress*, Vienna/Budapest, September

Siyan, K. & Hare, C., 1995, '*Internet Firewalls and Network Security*', New Riders, Indiana

Skillen, P., 1992, 'Desktop Data Security', *Computer Control Quarterly*, vol.10, no.1, pp 48-50

Skillen, P., 1991, Data Security on the Desk Top, *Proceedings of EDPAC '91*, Canberra, May, pp 455-478

Slayden P., 1993, Information Security Management, Business Information Security: First Line of Business Defence, *Proceedings of the Fourth South Pacific Region Security Conference,* 1-3 June, Melbourne, Australia

Smith, A.R., 1993, 'The Filter Model of Information Security: A Conceptual Model for Education and Training', in Dougall E.G. & Jones D. (eds), *Computer Security: Discovering Tomorrow,* Proceedings of the Ninth IFIP International Symposium on Computer Security, IFIP SEC '93, 12-14 May, Ontario, Canada, pp 53-67

Smith, E. & Eloff, J., 1998, 'Modelling Risks in a Health-Care Institution', *Proceedings of the XV IFIP World Computer Congress*, Vienna/Budapest, September

Smith, G., 1991, Incorporating Audit Requirements During Application Development, *Proceedings of EDPAC '91*, Canberra, May, pp 479-496

Smith, M., 1998, 'Security – Who Cares?', *Computer Fraud & Security*, April, pp 12-15

Smith, M.F. 1996, 'Data Protection, health care and the new European directive', *British Medical Journal*, vol 312, January, pp 197-198

Smith, P, 1970, '*Industrial Intelligence and Espionage*', London Business Books, London

Sobol, M. 1989, "Audit and Control of Microcomputers", *The Password*, August, pp 6-9

Sommer, P. 1993, 'Computer-Aided Industrial Espionage', *Proceedings of the Tenth World Conference on Computer Security, Audit and Control*, COMPSEC '93, London, May, Elsevier Advanced Technology, pp 334-342

Southee, D.W., 1992, 'Ethics in the Development and Application of Accounting Standards', *Proceedings of the Inaugural Series of Lectures in Business Ethics*, Curtin Business School, Curtin University of Technology, Perth, Western Australia, pp 29-40

Sprague R. and McNurlin B. (Ed's) 1986, "*Information Systems Management in Practice*" Prentice-Hall, Englewood Cliffs, New Jersey

Stallings, W., 1995, '*Network and Internetwork Security: Principles and Practice*', Prentice-Hall, Englewood Cliffs, New Jersey, USA

Standen, P. 1995, 'Enabling Organisational Learning with Qualitative Research', in '*Qualitative Research: Beyond the Boundaries*' conference proceedings, 21-22 November, Fremantle, Western Australia

Stang, D. and Moon, S., 1993, '*Network Security Secrets*', IDG Books, Massachusetts

Stanley, A., 1993, Pragmatic Security in Systems Development - a European Approach, *Proceedings of Tenth World Conference on Computer Security, Audit and Control*, London, October, pp 473-482

Stanley P. 1989, "Computer Crime Investigation - The Lessons Learned from Experience", in Grissonnanche (Ed), "*Security and Protection in Information Systems*", Elsevier Science Publishers, pp 297-305

Stannard, B. 1993, 'Doing the Right Thing', *Australian Business Monthly*, March, pp 33-35

Stemman R. 1987, "The Hidden Face of Fraud", *Business Computing & Communications,* September, pp 34-36

Sterling, B., 1992, "The Hacker Crackdown: Law and Disorder on the Electronic Frontier", Penguin Books, England

Stern, D. L., 1993, *Preventing Computer Fraud*, McGraw-Hill, New York

Stoll, C., 1989, "The Cuckoos Egg", The Bodley Head, London

Straub, D.W. and Carlson, C.L. 1989, 'Validating Instruments in MIS Research', MIS Quarterly, June, pp 146-165

Straub, D.W. and Hoffer, J. 1988, 'Computer Abuse and Computer Security Administration: A Study of Contemporary Information Security Methods', IRMIS Working Paper #W801, Indiana University, Indianapolis

Straub, D.W. and Nance, W. 1990, 'Discovering and Disciplining Computer Abuse in Organisations: A Field Study', *MIS Quarterly*, March, pp 44-60

Straub D. and Widon C., 1984, 'Deviancy by Bits and Bytes: Computer Abusers and Control Measures', in Finch J. and Dougall E. (Eds) '*Computer Security: A Global Challenge*', Elsevier Science Publishers, North-Holland, pp 91-102

Strous, L., 1994, 'Security Evaluation Criteria', Computers & Security, Vol. 13, pp 379-384

Sundt, C.E. 1994, 'The IBAG Framework for Commercial IT Security', in *Proceedings of the second Computer Security Conference, Singapore*, July, Singapore Institute of Management, Singapore

Swepson, P. & Dick, B. 1993, 'Action Research: Too Risky for Theses?', *Unpublished paper presented at the Social Psychologists Meeting,* Newcastle, April

Tait, P. & Vessey, I., 1988, 'The Effect of User Involvement on Systems Success: A Contingency Approach', *MIS Quarterly*, March, pp 90-107

'Targetting Fraud' 1989, *Directions in Government*, June, Australia, pp 40-41

Thomas, L.F. & Harri-Augstein, S., 1991, 'Conversational Measures of Effectiveness for Personal and Organisational Growth', in *Action Learning for Improved Performance*, Ed Zuber-Skerritt, AEBIS Publishing, Brisbane, Australia

Thomsett, R. 1993, 'Professionalism: A Question of Ethics', *Proceedings of the Symposium Virtual Ethics in the Age of Computing, Canberra, Australia*, March, pp 35-39

Thomson, M., 1999, 'Making Information Security Awareness and Training More Effective', in Yngstrom and Fischer-Hubner, (Ed's), '*WISE 1*', Proceedings of the IFIP TC11 WG11.8 First World Conference on Information Security Education, Stockholm University, pp 261-270

Tiley, E., 1996, "Personal Computer Security", IDG Books Worldwide Inc, Foster City, CA, USA

Treacher, A. and Bleumer, G., 1996, 'An Overview of SEISMED', in Barber, Treacher & Louwerse, (Eds), "*Towards Security in Medical Telematics*", IOS Press, Amsterdam, pp 4-9

Troy, E.F., 1989, 'Addressing the Telephone Intrusion Threat', in Grissonnanche (Ed), '*Security and Protection in Information Systems*', Elsevier Science IFIP, Holland, pp 55-65

Truman G., 1993, 'Harris First to Receive US Government Approval for Secure Networked Computer', *Business Wire*, September 20, p 1

UK Audit Commission, 1994, '*Opportunity Makes a Thief, An Analysis of Computer Abuse*', Audit Commission, UK, London

UK Audit Commission, 1998, '*Ghost in the Machine*', Bookpoint Ltd, Oxon UK

Usher, M. & Salus, I., 1998, 'Information Security Issues in an Age of Converging Technologies', *Computer Fraud & Security,* September, pp 16-19

Vasarhelyi, M. & Lin, T., 1988, *'Advanced Auditing Fundamentals of EDP and Statistical Audit Technology'*, Addison-Wesley, Reading Massachusetts, USA

Vassilacopoulos, G., Chrissikopoulos, V. and Peppes, D., 1996, 'Security Enforcement in a European Medical Device Vigilance System Network', in Katsikas, S. and Gritzalis, D. (Ed's), "*Information Systems Security*", Chapman and Hall, London, pp 377-386

Vaughn R., Saiedian H. & Unger E., 1993, 'A Survey of Security Issues in Office Computation and the Application of Secure Computing Models to Office Systems', *Computers & Security*, vol 12 No. 1, pp 79-97

Vitalari, 1983, "A Critical Assessment of Structured Analysis Methods: A Psychological Approach", in Bemelmens 1983, op cit

von Solms, S.H., 1996, 'Information Security on the Electronic Superhighway', in '*Information Systems Security*', Katsikas S.K. & Gritzalis D. (eds), Chapman & Hall, London, pp 153-166

Vorrath H. 1989, "Getting on Top of the End-User", *Computer Control Quarterly*, Vol 7, No 2, pp 31-35

Wallich P., 1994, Wire Pirates, *Scientific American*, March, pp 72-80

Ware, E., 1991, Securing the 90's Technology - Local Area Networks, *Proceedings of EDPAC '91*, Canberra, May, pp 531-541

Warman, A.R., 1993, '*Computer Security within Organisations*', McMillan, London

Warren, M., Furnell, S. and Sanders, P., 1997, 'ODESSA: A New Approach to Healthcare Risk Analysis', in Yngstrom, L. & Carlsen, J. (Ed's), 'Information Security in Research and Business', Chapman & Hall, London, pp 391-402

Watne, D. and Turney, P., 1990, "*Auditing EDP Systems*", Prentice-Hall, Englewood Cliffs, New Jersey

Watson, R., 1989, "Key Issues in Information Systems Management: An Australian Perspective - 1988", *The Australian Computer Journal*, Vol 21, No 2, August, pp 118-129

Watson, R., Kelly, G., Galliers, R. & Brancheau, J., 1997, 'Key Issues in Information Systems Management: An International Perspective', *Journal of Management Information Systems*, vol. 13, no. 4, pp 91-115

Weick, K.E. 1984, 'Theoretical Assumptions and Research Methodology Selection', in F.W. McFarlan (Ed), 'The Information Systems Research Challenge', Harvard Business School Press, Boston, Massachusetts, pp 111-132

Weiss, K.P., 1992a, 'Security Tokens or 'Token' Security?', *Computer Control Quarterly,* vol.10, no.3, pp 6-11

Weiss, K.P., 1992b, 'Security for Today's and Tomorrow's LAN-Linked Information Resources', *Computer Control Quarterly,* vol.10, no.3, pp 45-55

White, K.B., 1984, 'MIS Project Teams: An Investigation of Cognitive Style Implications', *MIS Quarterly*, vol. 8, no. 2, June, pp 95-101

White, G.B., Fisch, E.A. & Pooch, U.W., 1996, *'Computer System and Network Security'*, CRC Press Inc, Boca Raton, Florida, USA

Wiener, L.R., 1993, "Digital Woes: Why we should not depend on software", Addison-Wesley, Reading, Massachusetts, USA

Will, H.J., 1992, 'Why We Cannot Trust Computer Systems - and What This Means for IS Auditors', *Proceedings of EDPAC 92*, Adelaide, Australia, May 20-22

Wilsher, R.G., and Kurth, H., 1996, Security Assurance in Information Systems, in Katsikas, S. and Gritzalis, D. (Ed's), "*Information Systems Security*", Chapman and Hall, London, pp 74-87

Wilson, B., 1990, *'Systems: Concepts, Methodologies, and Applications'*, John Wiley & Sons, Chichester, UK

Wilson, K., 1991, Effectively Managing the Software Development Lifecycle, *Proceedings of EDPAC '91*, Canberra, May, pp 555-560

Wilson, J.L., Turban, E., Zviran, M. 1992, 'Information Systems Security: A Managerial Perspective', *International Journal of Information Management*, vol. 12, pp 105-119

Wolfe, H.B., 1995, 'Computer Security: For Fun and Profit', *Computers & Security*, vol. 14, pp 113-115

Wood, C.C., 1992, 'To Guess or Not to Guess', *Computer Control Quarterly*, vol.10, no.1, pp 35-38

Wood, C.C., 1995 'Writing InfoSec Policies', *Computers & Security*, Vol. 14, No. 8, pp 667-674

Wood, C., Banks, W., Guarro, S., Garcia, A., Hampel, V. & Sartorio, H., 1987, *'Computer Security A Comprehensive Controls Checklist'*, John Wiley & Sons, New York

Wood, M., 1982, *'Introducing Computer Security'*, NCC, UK

Woog, R. and Turner, T. 1992, 'Improving Agricultural Extension through Action Research Education', *Proceedings of the Second World Congress on Action Learning*, July, Brisbane, pp 105-108

Wrycza, S. and Plata-Przechlewski, T., 1994, 'Key Issues in Information Systems Development. The Case of Poland', in Zupancic J, Wrycza S. (Eds) *Proceedings of the Fourth International Conference on Information Systems Development ISD'94*, Bled, September, pp 289-296

Yadav, S., Bravocco, R., Chatfield, A. & Rajkumar, T., 1988, 'Comparison of Analysis Techniques for Information Requirements Determination' *Communications of the ACM,* September, vol. 31, no. 9, pp 1090-1097

Yaverbaum, G., 1989, 'Specifying Systems Requirements: A Framework of Current Techniques', *Journal of Information Systems Management*, Winter, pp 17-21

Yin, R.K., 1989, 'Research Design Issues in Using the Case Study Method to Study Management Information Systems', *Harvard Business School Research Colloquium*, Harvard Business School, Boston, MA, USA

Yngstrom, L., 1995, 'A Holistic Approach to IT Security', *Proceedings of IFIP SEC '95, South Africa,* May, pp 98-109

Yngstrom, L., 1996, 'IT Security and Privacy Education', , in Katsikas, S. and Gritzalis, D. (Ed's), "*Information Systems Security*", Chapman and Hall, London, pp 351-364

Yngstrom, L. and Bjorck, F., 1999, 'The Value of Assessment of Information Security Education and Training', in Yngstrom and Fischer-Hubner (Eds), *'WISE 1 – Proceedings of the IFIP TC11 WG11.8 First World Conference on Information Security Education*', Stockholm University, Sweden, pp 271-292

Yui, K. & Tse, Y.Y., 1995, 'A Model for Disaster Recovery Planning', *IS Audit & Control Journal*, vol. V, pp 45-51

Zuckerman, M., 1998, 'Moving Towards a Holistic Approach to Risk Management Education – Teaching Business Security Management', *Security Journal,* vol. 11, pp 81-89

APPENDIX A

RECOMMENDED SECURITY PRACTICES

APPENDIX A - RECOMMENDED SECURITY PRACTICES

A.1 Corporate Security Policy

Just under half of the respondents in the NCC (1994) study were reported to have not implemented a formal information technology security policy. The first step towards effective security management involves commitment by the senior executive in the form of an information security policy. This policy must be issued by senior management as this is where responsibility ultimately rests (Devargas 1993; Elbra 1992; Wood et. al. 1987; UK Audit Commission 1994). It is important that the policy be issued organisation-wide to ensure consistency across different departments or sections (James and Chantler 1993a). The corporate security policy must be relevant to information in all its forms (verbal, handwritten and electronic), in all its environments, not just computer systems and throughout its life-cycle (Bentley, Hinde and Oliphant 1995; Wood et. al. 1987).

To enable the organisation to fulfil its mission, the corporate information security policy needs to be based upon organisational objectives and be integrated with business strategies (Devargas 1993; Fink 1997; Hoppe 1994; Markey 1989; UK Audit Commission 1994; Warman 1993). The integration of an information security policy with other organisational plans at all levels is illustrated in Figure A.1. The link between strategic planning and security policy is a two-way flow with the security policy also influencing organisational plans at lower levels.

The information security policy should include:

1. Broad aims and objectives of security for the organisation's information, e.g. confidentiality, availability, integrity, authenticity, etc. (Blair 1991; Elbra 1992; Ernst and Young 1993; James and Chantler 1993a)
2. Legal or statutory requirements including privacy, data protection, copyright, patents and the like (Elbra 1992)
3. Classification of information, appropriate action for each class and ownership responsibilities (Blair 1991; DOCIT 1988; Elbra 1992; Wood et. al. 1987)
4. Statements of responsibility for security for all levels of employees (Blair 1991; Devargas 1993; Elbra 1992; Ernst and Young 1993; James and Chantler 1993a;

Wood et. al. 1987). It should also be made clear that all staff will be held responsible for non-compliance (Elbra 1992) and include action that will be taken for such failure to comply (Wood et. al. 1987).

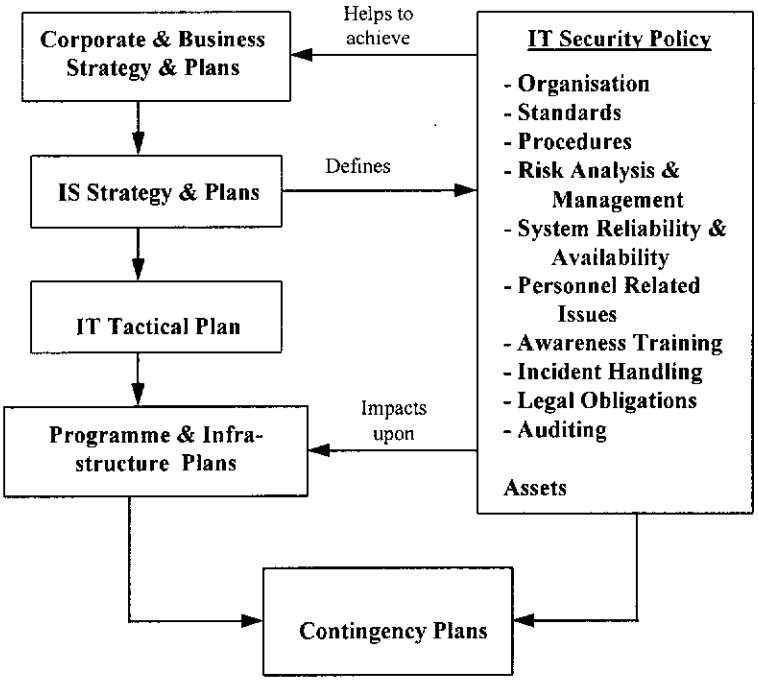

Figure A.1: Integration of Information Security Policy with Organisational Plans (source: Devargas 1993:8)

The information security policy should:

1. Be a high level document that does not contain detailed standards and procedures (Baskerville 1988; Elbra 1992).
2. Not reference specific technological platforms or organisation structures (DOCIT 1988; James and Chantler 1993a). This will ensure the policy is generic in nature and any changes in technology or minor management structure will not necessitate changes to the policy.
3. Be succinct and short enough to be widely distributed and read by all staff (Baskerville 1988; Devargas 1993; DOCIT 1988; Elbra 1992; Markey 1989).

4. Become the basis of an education and awareness program (DOCIT 1988; James and Chantler 1993a; O'Donoghue 1987).

Recommended contents and examples of corporate security policies can be found in Baskerville (1988:38), Bentley, Hinde and Oliphant (1995), Devargas (1993), DOCIT (1988:89), Elbra (1992), Principal Financial Group (1999), Sawicki (1992:328) and UK Audit Commission, (1994:29). In addition, more than 500 information security policies are illustrated in a book titled "Information Security Policies Made Easy" on the Internet at [*infosec@baselinesoft.com*].

Additional discussion and recommendations relating to corporate information security policies are to be found in Baskerville (1997b), Chantico (1992), Curry (1992), Duncan (1995), Ernst and Young (1998), Fagan (1993), Forcht (1994), Lane (1985), Lindup (1995), Main (1995), Newman (1993), O'Donoghue (1987), Otway (1992), Parker (1981) and Purser (1993).

A.2 Information Security Planning and Budgeting

An information security plan should address all major issues relating to the security of the organisation's information, upholding the information security policy. The security plan should include aims and scope of the plan, and its links with other management plans, such as contingency plans, etc. (James and Chantler 1993a; Devargas 1993); results of security reviews and planned activities to be carried out, resource requirements for each activity (e.g. personnel, skills, time, equipment), budgetary details, benefits to be achieved and assigned responsibilities (James and Chantler 1993a).

DOCIT (1988:10-12) gives guidance for developing a security program and recommends action be undertaken at three stages. At the design stage: establish technical requirements, devise risk management alternatives, create cost estimates, undertake security audits and evaluations, involve end-users in planning, make specifications, evaluate devices, and prepare necessary contracts. At the implementation stage: integrate user needs and technical requirements, organise

technical teams, co-ordinate program phases, test the effectiveness of existing and planned security. At the operational stage: create security awareness training programs, establish means to place security within all corporate levels, establish measures of security awareness, determine the willingness and ability of an individual employee to comply with security requirements, and review the detection system for computer crime and abuse.

An information security plan must emphasise corporate-wide participation (Hoppe 1994; Markey 1987) as implementation of the plan is intended to change the corporate culture. It is therefore necessary for all staff members to participate and accept responsibility for security. The objectives of such a plan must be sold to each management level in a form which is understood at that level, as "bolts of lightning thrown down from Olympian ivory towers are never popular and rarely successful" (Hoppe 1994:28). Additional recommendations for security planning and budgeting are contained in Baskerville (1997), Benbow, Masters and Cooper (1986), Bergman (1991), Connolly (1990), Forcht (1994), Lane (1985), Otway (1992) and Wood (1995).

A.3 Risk Analysis

There is a wealth of literature supporting risk analysis methods and the need for management to undertake risk analysis with regard to information systems security. For example, in addition to those sources quoted below, further support for the risk analysis process can be found in Baskerville (1996 and 1997), Bhaskar (1993), Dacier, Deswarte and Kadniche (1996), Elbra (1992), Ernst and Young (1993 and 1998); Grant (1991); Klosky, Gallegos and Klosky (1995), Labuschagne and Eloff (1996), Purser (1993), von Solms (1996), Warman (1993). However, it is interesting to note that a study by the NCC (1994) reported that only 43% of participating organisations undertook a formal risk analysis process.

The risk analysis process commonly consists of the following steps:

1. Identification of assets (including information)
2. Identification of associated threats
3. Analysis of risk exposure associated with each asset

4. Cost justification and selection of security measures to counteract the threats
5. Implementation and evaluation of security measures

(Bhaskar 1993; Bergman 1991; DOCIT 1988; Ekenberg, Oberoi and Orci 1995; Jackson and Hruska 1992; James and Chantler 1993a; Lane 1985; Pfleeger 1997)

Unfortunately, risk analysis can be confusing, according to Bentley, Hinde and Oliphant (1995), as there are no generally accepted approaches or terminology in the area. Risk analysis approaches are frequently categorised into either quantitative or qualitative (DOCIT 1988; Forcht 1994; Fink 1997). Quantitative risk analysis provides management with a specific dollar loss expectancy on which to base counter measure considerations. However, this method is time consuming and expensive, and the results may be misinterpreted due to the complexity of the process. Quantitative approaches may lead to several different conclusions based on the same data (DOCIT 1988). Qualitative risk analysis utilises analysis based upon groupings and ratings rather than mathematical formula. Hence it is more informal and usually requires less time and fewer resources. A qualitative risk determination model is presented in Figure A.2 illustrating the ratings of impact of risks and the probability of occurrence.

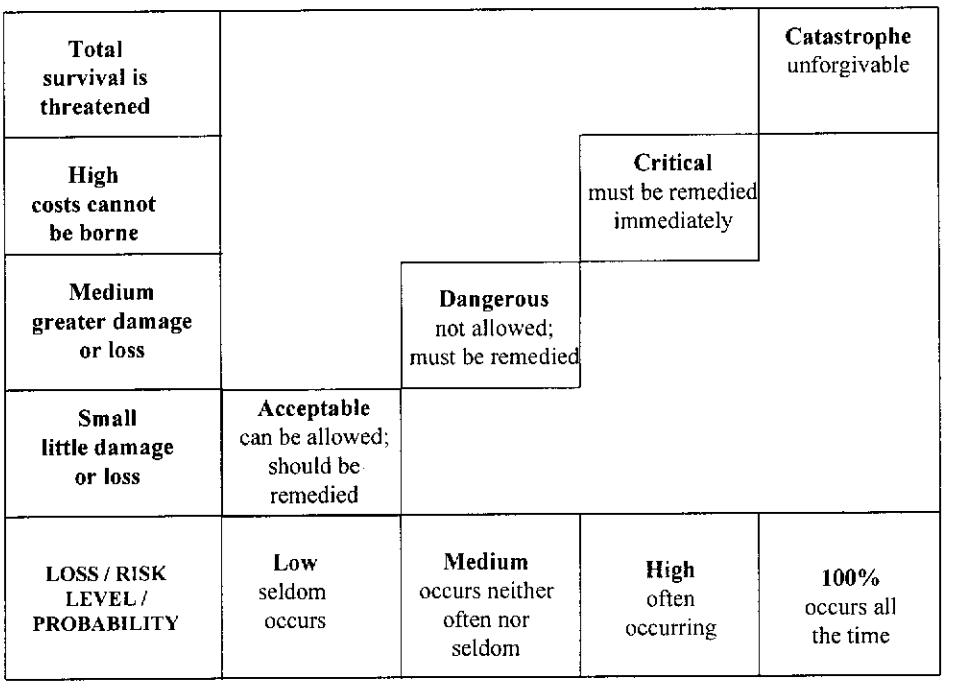

Figure A.2: Qualitative Risk Determination Model (source, Fink 1997, page 25)

Regardless of the approach taken, it is advisable to undertake risk assessment proactively, rather than reactively (Icove, Seger and von Storch 1995).

A.4 Information Classification and Ownership

As organisations have become more reliant upon information and information systems for continued business success, so the need for classification of information has grown. The main reason for classification of information is to assign responsibility for that information, provide guidance for its use and analyse requirements regarding its confidentiality, integrity and availability (Ernst and Young 1993). The process of classification also aids management in deciding what to protect and how much ought to be spent on protecting it (Alexander 1996).

There are numerous classification systems recommended by researchers and authors in the information security field and very few of these are alike. DOCIT (1988) recommends four classifications; *public*, being open or unclassified, *confidential*, being proprietary or internal use only, *personal*, being personnel data and *restricted*, where distribution is restricted to specified individuals. The military four-level model is suggested by Carroll (1996) comprising *top secret*, *secret*, *confidential* and *restricted* classifications for information. Adaptation of the military model also uses a four part classification comprising *unclassified* for public access, *private* for use within the organisation, *confidential* for restriction access within the organisation, and *secret* covering the organisation's most sensitive information (Alexander 1996).

A six-level model for the classification of information includes levels restricted to *named individuals*, restricted to *named departments or sections*, restricted to those with a *standard of 'security clearance'*, restricted to *specified management levels*, limited to *internal use* and *no limitation* as to use (Elbra 1992).

Forcht (1994) suggests information falls into seven categories; *competitive-edge,* designs, client lists, pricing, *confidential operational,* future plans - prospective clients, advertising campaigns, takeover strategies, *privacy-based confidential,* payroll, supplier and customer info, *critical operational,* reference files, price lists,

instruction sets, *high cost information,* extensive investment such as research, *fraud potential data,* material with potential financial benefits, and *security data,* access files and keys, encryption algorithms.

As there appears to be no one recommended system of classification, each organisation must devise and use an appropriate classification for its particular needs.

In addition to the classification of information, it is also necessary to identify the role staff members have to play with regard to that information. The three roles generally assigned are owner, custodian and user (DOCIT 1988).

1. Information Owner - A person or manager of an organisational entity which creates the information or who most directly benefits from the existence of the information in performing their function.
2. Information Custodian - a person or organisational entity with responsibility for the safekeeping of information owned by others.
3. Information User - a person or organisational entity who makes use of information owned by others in performing their functions.

There are specific responsibilities that come with each of these roles as illustrated in Table A.1. As the responsibility for information is commonly held by the IS department (either by design or by default) ownership of an organisation's information is assumed to reside with that section. However, the IS section generally takes the information created by others and makes it available to staff members to use in performing their given functions. The IS section does not create information and so should not be the owner, but the custodian of information it handles (DOCIT 1988; Forcht 1994).

Further discussion on the need for information classification and assignment responsibility via roles is also supported by Baskerville (1997b), Bergman (1991), Blair (1991), Chantico (1992), CSI Roundtable (1998), Hoppe (1994), Kwok and Longley (1997), Lane (1985), Parker (1981), Peltier (1998), Schwartau (1996), Sobol (1989), Wood M. (1982), Wood C.C. (1995) and Wood et. al. (1987).

OWNER	CUSTODIAN	USER
- identifying information - acknowledging ownership - classifying information - specifying business controls - authorising access - approving application controls and security measures - participating in risk assessment - undertaking contingency planning	- safekeeping of information - follow-up of violations - investigating loss of integrity - participation in contingency planning	- compliance with standards, procedures and guidelines - safeguarding security authentication - non-disclosure of information - responding to security violations

Table A.1: Security Responsibilities for Information (compiled from Alexander 1996; Corby and Johnston 1998; DOCIT 1988 and Forcht 1994).

A.5 Contingency Planning

The reason for disaster recovery planning is to minimise disruption to the organisation's operations caused by a contingency. The need for contingency planning increases with the organisation's increased reliance upon computerised information systems, with exposures including risk of financial loss, legal responsibility and interruption to business service (Chantico 1985). Disaster recovery planning is an organisational responsibility and IS disaster recovery planning should be only one part of the organisation's overall disaster recovery plan (Yiu and Tse 1995)

Recommended steps in the disaster recovery planning process include:

1. Undertake risk analysis
2. Analyse critical data and applications
3. Appointment of a disaster recovery co-ordinator,
4. Off-site storage of critical data

5. Formulation of emergency and recovery strategies, including backup sites
6. Document the plan
7. Testing of the plan
8. Maintenance of the plan

(Chantico 1985; DOCIT 1988 and 1989; Fink 1997; James and Chantler 1994; Yui and Tse 1995)

The recommended components of a disaster recovery are illustrated in Figure A.3 and include definitions, a backup plan, recovery plan, test plan and a maintenance plan.

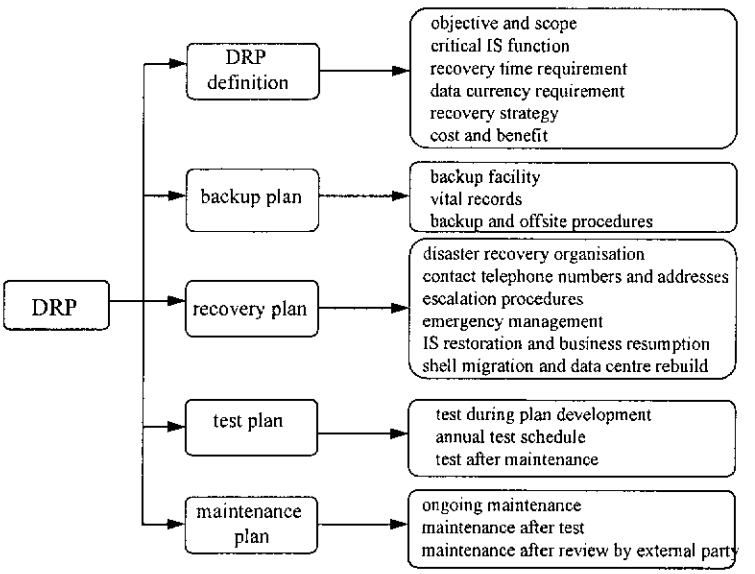

Figure A.3: Components of a Disaster Recovery Plan (source: Yui and Tse 1995)

The increased need for disaster recovery planning, particularly in networked environments, is expoused by Baker (1995), Corrigan (1994), Davis (1994), Hopkinson (1992b), and Stang and Moon 1993. Further discussion on disaster recovery and the contingency planning process can be found in Baskerville (1988 and 1997b), Benbow, Masters and Cooper (1986), Bergman (1991), Chantico (1985), Ernst and young (1998), Forcht (1994), Hoppe (1994), Klosky, Gallegos and Klosky

(1995), Lane (1985), Parker (1981), Sobol (1989) and Wood, (1982). Despite these recommendations for disaster recovery planning, NCC (1994) found only 59% of organisations study had established contingency plans, and 40% of these did not test them regularly.

A.6 Security Manager and Active Supervision of Security

Lack of management and inadequate supervision of information security are contributing to the increase in information security problems (Chantico 1992), with the organisation's ability to implement effective information security strategies being hampered due to lack of consistent security responsibility assignment (Duncan 1995). A study carried out by the NCC (1994) reported that only 15% of respondents had a specialist security function in place.

The responsibility for security management must be assigned to a person in authority (Baskerville 1988; Blair 1991; James and Chantler 1993a). Such a person needs to have the knowledge and experience to handle this area effectively, as well as the time, finances and ability to actively supervise information security matters (Blair 1991; James and Chantler 1993a). This role will be most successful where there is a high level of visible supervision - regular reviews of procedures, investigation of error reports, system logs, audit reports and complaints, and follow-ups to ensure the required action has been taken. Hence the security manager's role should be clearly defined with regard to the area, the scope and the level of responsibility (Baskerville 1988:41). It is also important that employees know who to approach in the event of questions, discovered vulnerabilities and suspected abuse (James and Chantler 1993a).

Support for the security manager function can also be found in Baskerville, (1997b), Benbow, Masters and Cooper (1986), Edwards (1991), Fagan (1993), Forcht (1994), Hoppe (1994), Klosky, Gallegos and Klosky (1995), Lane (1985), Parker (1981) and Wood (1995).

A.7 Security Education and Training

Employees cannot be expected to share the same concern as management with regard to security if they are not aware of the need for security. Information security procedures need to flow through the organisation and employees need to be aware of these procedures (Newman 1993; Thomson 1999). One of the most effective means of raising security awareness within organisations is to conduct information security education for all employees (Baskerville 1997b; DOCIT 1988; Edwards 1991; Elbra 1992; Fink 1997; James and Chantler 1993a; O'Donoghue 1987; Warman 1993).

Training and education in security and standards particularly where organisations use contemporary tools and networked development environments is also important (Fitzgerald 1985 and 1990; Gerrity and Rockart 1986; Harris 1988; James and Morien 1991 and Vorrath 1989). All employees should be encouraged to integrate security consciousness into their daily work (DOCIT 1988).

An information security education program should include:

1. Details of the organisation's policy on security - its aims and how it plans to achieve those aims (Fink 1997; James and Chantler 1993a; Markey 1989; Warman 1993)
2. Details of the security plan at an overview level to enable staff to see the full picture or scope of security for the entire organisation (James and Chantler 1993a)
3. Details of responsibility for security at all levels, highlighting the management and supervisory roles to illustrate active management support (James and Chantler 1993a; Markey 1989)
4. In depth details of the sections of the security plan which directly effect each employee and their areas of security responsibility (James and Chantler 1993a; Markey 1989)
5. These should be tailored to ensure they are appropriate for each level of employee (James and Chantler 1993a; Markey 1989)
6. Emphasis that security is an ongoing practice and regular reviews of security measures will be undertaken (James and Chantler 1993a)

7. Constant reminders of security issues on noticeboards around the office and organisational newsletters and the like (James and Chantler 1993a; Warman 1993)

Key features of the information security education program include:

1. Knowledge about security measures and processes should be issued on a need to know basis
2. Security education should be held for all new employees before they begin their employment, stressing in non-technical terms, the threats and vulnerabilities associated with information assets (Fink 1997; Markey 1989; Warman 1993)

Regarding the US Department of State's security education program Markey (1989:86) recommends written security responsibility assignments as they show exactly what each employee needs to know to do the job assigned to them. Where the content of the training is sharply focused on these needs, it is apparent to the employees and they are motivated to apply themselves and absorb the material. Upon gaining confidence in their ability to deal with information security matters, they become active participants in the program and incorporate security into their daily work patterns.

Additional recommendations relating to security awareness and education can be found in Chantico (1992), Ernst and Young (1998), Fitzgerald (1992a), Forcht (1994), Hoppe (1994), Lafleur (1992), Raab and Williams (1999), UK Audit Commission (1994) and Yngstrom (1996).

A.8 Software Quality Assurance and Security Standards

Information systems which have low quality software present a web of problems for the manager attempting to control illegal and unauthorised use, abuse and errors resulting from intentional or unintentional misuse (James and Chantler 1993a). Unfortunately, only a minority of organisations have an effective quality assurance function operating, if any at all (Benbow, Masters and Cooper 1986; James and Coldwell 1993).

Recommended quality features are summarised in Table A.2. These quality features include security aspects in general, however desirable information security features need to be specified and should include integrity, confidentiality, availability, authentication and non-repudiation of electronic transactions (Fink 1997).

ATTRIBUTES	CRITERIA	DESCRIPTION
CONFORMITY	Completeness Correctness Traceability	Does the product have the desired data, function and procedures as required
USABILITY	Completeness Operability Support Training Correctness	Is the product easy to use, learn and understand from the user's perspective
EFFICIENCY	Processing Network Storage	Does the application use the hardware, system software and other resources efficiently
MAINTAINABILITY	Structure/ Modularity Simplicity Commonality Documentation Self-descriptiveness	Is the system easy to maintain and correct
REUSABILITY	Self-descriptiveness Independence Structure/ Modularity Commonality Application Independence Simplicity	Does the system use code and data that is capable of being used by other systems
FLEXIBILITY	Structure/ Modularity Simplicity Documentation Self-descriptiveness	Is the system easy to enhance in order to add or modify function and data
RELIABILITY	Structure/ Modularity Correctness Simplicity	Does the system operate without failure and with consistency
PORTABILITY	Independence Simplicity Structure/ Modularity Self-descriptiveness	Is the system easy to migrate to another hardware, software environment
AUDITABILITY and SECURITY	Structure/ Modularity Access Control Audit Control	Is the system secure from unauthorised access and is it auditable
JOB IMPACT	Correctness Work Dimensions Support Operability Training Network Documentation	Does the system provide acceptable working environments for direct users

Table A.2: Software Quality Attributes (source: Thomsett 1993:171)

Alternatively, by using standards such as ISO 9000 as a basic structure, many organisations have been successful in improving their software processes and eliminating their quality related problems (Allen 1995). The adoption of international standards for information systems development has raised the importance of the quality function in business organisations. Quality assurance methodologies such as SQA2000 have been developed, based upon the Australian Standard AS3563 and the ISO 9000 series, to ease the implementation of quality procedures within organisations (Edelson and Parker 1995).

This has led to a call for the development of international information security guidelines (Strous 1994), with the many security standards under analysis including ITSEC in Europe, USA New Federal Criteria including TSSEC (commonly known as the Orange Book), CTCPEC in Canada and the ISO SC27 WG3 security evaluation criteria (Kruger and Eloff 1997; Purser 1993).

Other authors supporting the quality assurance function and use of written standards and procedures include Chantico (1992), Devargas (1995), Fillery (1996), Frangos (1996), Hopkinson (1992a), Hoppe (1994), Sapienza (1995a 1995b), and Wilsher and Kurth (1996).

A.9 Physical Controls

Physical controls are set in place to protect and restrict access to equipment, materials, software and data (Benton 1998; Madron 1992; White, Fisch and Pooch 1996). Physical security includes consideration of threats associated with environmental location, physical building, rooms or areas containing computers, servers, and other computer equipment, and the equipment itself.

Recommended security measures include fences, perimeter lighting, video surveillance, automatic alarm systems, security guards, personnel identification such as ID badges, supervision of visitors, vehicle access barriers and passes, man-traps, logging of staff activities within restricted areas by electronic access methods,

mechanical and electronic keys, fibre optics cabling, electro-magnetic radiation protection, and biometric devices such as retina scans, voice verification, finger or hand prints, signature dynamics (Bhaskar 1993; Carroll 1996; Fink 1997; Forcht 1994; Khandeker and Langer 1990; Madron 1992; Pfleeger 1997; Sobol 1989; Watne and Turney 1990; White, Fisch and Pooch 1996).

Consideration of potential physical assaults is necessary in the planning of physical security safeguards (Fitzgerald K. 1992c). Rated by strength of origin, Figure A.4 illustrates potential physical assaults and means of protecting against such attacks.

Strength	Probable Origin	Characteristics	Protection
1	Inquisitive pedestrian	Walking through open or unlocked doors	Locked or patrolled doors
2	Drunks and idle children	Uncoordinated manual force, low persistence	Locked or patrolled doors
3	Vandal and petty thieves	Moderate persistence, use of small implements	Looked doors, visibly patrolled or monitored
4	Unorganised trouble groups	Moderate attack, use of any handy implement of low penetration strength	Strengthened outer perimeter with sealable internal doors
5	Organised trouble makers	Low target knowledge, cohesive assault, probably at ground level	Strengthened and reinforced ground level perimeter, particularly doors. Access control by patrol or monitoring
6	Pre-planned single or group assault	A good knowledge of available information on the target, modest weaponry, possibly incendiary and scaling equipment	Strengthened and reinforced total perimeter, surveillance equipment, bullet-proof glass. Delaying type barriers
7	Financially backed single or group assault	Good knowledge of the target, advanced or bulk implements or subtle penetration tools or techniques	Heavily reinforced perimeter, high resistance doors, sophisticated access control. Security screening of personnel
8	High cost, well organised group assault	Excellent and complete knowledge of the target. Highly sophisticated penetration equipment and techniques	Army style defence force

Figure A.4: Potential Security Assaults (source: Fitzgerald, K 1992c:43)

In addition, generally recommended physical control measures can be found (Becker 1977; Bergman 1991; Chantico 1992; DOCIT 1988; Elbra 1992; Forcht 1994; Icove, Seger and von Storch 1995; Lane 1985; Parker 1981; Weiss 1992a; Wood 1982).

A.10 Logical Access Controls

The data and software needs to be secured, with the facilities accessible only to those who need it, restricting access to all files on a need-to-know principle (Ernst and Young 1993). Logical access controls encompass measures for user identification and authentication on entry to the system, and restriction of actions once access has been grained (Bhaskar 1993).

One can gain access to the system by providing *something one knows*, *something one has* and *something one is or can do* (Kurzban 1986). Logical access identification and authentication controls relating to *something one knows* include userid's, passwords, PINs and security codes. Controls for *something one has* include smartcards, password generating software and hand-held authentication devices. *Something one is or can do* controls embrace biometric and biogenic devices such as scans of the retina, face or hand; prints of the finger, hand or other body parts; signature dynamics; voice recognition and saliva analysis.

Logical access controls generally limit a user's activities in the reading, writing, executing, cataloging and other uses of data and systems resources (Wood et. al 1987). In addition, different users need to be logically separated so that they can only access particular programs or information (Bhaskar 1993; Gasser 1988; Harmon 1998). Security measures to assist in the restriction of action once access to the system has been granted include restriction by user group classification, restriction of system objects (files, etc) by type or group, access control lists, tables and matrices, and other differentiated access rights (Gasser 1988; James and Chantler 1993a; Pfleeger 1997). Access control tables and matrices restrict addition, modification, deletion and execution actions to those specified for a given user. Such access rights for each user can be differentiated by transaction types, workstation or device location and address, and time of day (James and Chantler 1993a; Watne and Turney 1990).

To be effective logical access controls need to be mandatory for all employees, an integral part of normal working procedures and require minimal supervision (DOCIT 1988).

Guidelines for the use and management of passwords are detailed in Cairo and Friedberg (1995), Forcht (1994), Hains (1992b), Jackson and Hruska (1992), James and Chantler (1994), Pfleeger (1989), Tiley (1996), UK Audit Commission (1994), Watne and Turney (1990), Weiss 1992a, Wood (1992) and Wood et. al. (1987).

Additional authors and researchers highlighting the need for logical access controls include Anderson, (1972), Bergman (1991), Chantico (1992), Fink (1997), Fitzgerald (1990), Forcht (1994), Hains, (1992b), Harris (1988), Holbein et. al. (1997), James and Morien (1991), Khandeker and Langer (1990), Lane (1985), Parker (1981), Sobol (1989), Weiss (1992a) and Wood (1982).

A.11 System Logs and Audit Trails

System logs and audit trails provide a record of user and processing activities occurring on a computer system. These logs are required in order to trace user activities as well as the processing and disposition of all entered transactions (Moeller 1989; Wood et. al. 1987). System logs and audit trails are designed to encourage users to remain accountable for their actions whilst using the system and information (Weiss 1992a).

Systems software for large computer systems and networks commonly include automatic logging programs for this purpose. However tracing activities on PCs and small networks can be difficult if logging facilities are not in operation. Due to the higher risks to integrity, availability and confidentiality in PC and networked systems, automatic logging is desirable (Cooper et. al. 1995; Kwok and Longley 1997). System logs of user activities need to detail the identification of the user, time and day of access, and details of actions performed (Baker 1995; Forcht 1994; Garfinkel and Spafford 1991; Stang and Moon 1993). The audit trail of transactions provides information on the initiation, authorisation, approval and recording of

transactions processed (Watne and Turney 1990). User activity logs, in particular, must be constantly monitored and reviewed (Bhaskar 1993; Forcht 1994). Users who are knowledgeable about system features can access and modify these logs (Clough and Mungo 1992; Hafner and Markoff 1993; Sterling 1992; Stoll 1989), thus adequate security measures to restrict the modification and deletion of entries in such logs is also recommended (Wood et. al. 1987). Because systems logs and audit trails of user and processing activities form an essential base for the audit functions in and around computerised information systems the integrity of logs must be ensured (Bhaskar 1993).

The need for system logs and management of audit trails is presented by numerous additional authors, including Anderson (1972), Bentley, Hinde and Oliphant (1995), Chantico (1992), Curry (1992), Elbra (1992), Fink (1997), Fitzgerald (1990), Hains (1992b), Harris (1989), James and Morien (1991), Khandeker and Langer (1990), Lane (1985), Neumann (1995), O'Neil-Dunne (1990), Smith (1991), Sobol (1989) and Tiley (1996).

A.12 Change Control

Written procedures to monitor and manage the modification of operational programs should be in place to ensure ongoing system security (Moeller 1989). These procedures need to cover the approval and authorisation of proposed changes, their subsequent testing and implementation, plus the update of related systems documentation (Martin 1992; Vasarhelyi and Lin 1988; Watne and Turney 1990). Changes to programs need to be limited to authorised personnel and all activities logged in audit trails for review (Martin 1992; Moeller 1989; Vasarhelyi and Lin 1988). A good change control program should work to prevent unauthorised or undocumented changes to computer programs before these changes are relied upon to perform business functions.

A.13 Security Reviews and Audits

Sound internal audits ensure that all staff work in a well-regulated environment which minimises the opportunity for any member of staff to commit a fraud, and the internal computer audit provides an essential ingredient in the internal control

mechanism (UK Audit Commission 1994). To be effective the audit or security review must be carried out at regular intervals, on an annual basis as a minimum (DOCIT 1988; Kwok and Longley 1997). This regular review is designed to ensure all the necessary security measures are effectively in place as well as determining the necessity of measures based upon reviews of risks (Davis 1994).

A strategy of many organisations in leading edge technology is to conduct unannounced audits. Regular reviews and audits are recommended to be carried out by independent staff or auditors (Forcht 1994; James and Chantler 1993a). In addition, the auditor needs to design, or at least review, procedures for building adequate controls into systems, in addition to reviewing the coverage of quality control (Fitzgerald 1990; James and Morien 1991; Khandeker and Langer 1990).

Additional discussion on security reviews and audits can be found in Bhaskar (1993), Benbow, Masters and Cooper (1986), Bentley, Hinde and Oliphant (1995), Bergman (1991), Chantico (1992), Fagan (1993), Fink (1997), Moeller (1989), Neumann (1995), Parker (1981), Sapienza (1995b), Vasarhelyi and Lin (1988) and Watne and Turney (1990).

A.14 Backup and Recovery Procedures

Backup and recovery procedures are required to ensure ongoing file and system integrity and availability (Moeller 1989; Stang and Moon 1993). As the sex appeal of backing up software and data is not great (Tiley 1996) and is often seen as a loathsome task (Davis 1994), written backup and recovery procedures are helpful.

The process of backing up needs:

(a) to be carried out regularly (Bhaskar 1993; Fink 1997; Wood et. al. 1987)

(b) storage of backup media in a secure place, with copies kept both on-site and off-site (Bhaskar 1993; Carroll 1996; Denning 1990; Fink 1997; Forcht 1994; Stang and Moon 1993)

(c) regular testing of backups to ensure they are readable and virus free (Denning 1990; Garfinkel and Spafford 1991; Stang and Moon 1993).

Most organisations underestimate possible events that can cause power failure or power cut-off to their computers and communications systems. Hence a backup power supply is recommended in the form of a UPS (uninterrupted power supply) unit (Alexander 1996; Carroll 1996; Cowcher 1992; Pearson 1992; Stang and Moon 1993).

For further discussion on backups see Anderson (1972), Baskerville (1997a), Benbow, Masters and Cooper (1986), Curry (1992), Edwards (1991), Forcht (1994), Hains (1992b), Harris (1988), James and Morien (1991), Khandeker and Langer (1990), Leveson (1995), Pfleeger (1997), Watne and Turney (1990) and Wiener (1993).

A.15 Network and Communication Controls

Networks are predominantly collections of PCs, workstations, and servers, yet have the power of mainframes and minicomputers. Due to their structure and composition, networks and distributed systems pose greater security risks than traditional centralised systems (Davis 1994; Hancock 1998; James and Chantler 1993ab; Kogan, Sudit and Vasarhelyi 1996; Moignard 1995; Pfleeger 1997; Sawicki 1992; Usher and Salus 1998; Ware 1991). In particular, networks are risks for three reasons; more points of access exist, the physical perimeter of the computer system is extended and more services are offered to users (Cheswick and Bellovin 1994).

Security measures recommended in this appendix for all types of systems are particularly applicable in networked environments. These controls include security policies; physical security of computer hardware (workstations, servers, communications equipment, etc.) and the building; logical access controls for all software and data; audit trails and system logs of activities and processing; encryption of data and messages; risk assessment and security planning; contingency planning; backup and recovery procedures; information classification and ownership;

security awareness and training; network security management and supervision; virus and worm protection (Cooper et. al. 1995; Corby and Johnston 1998; Corrigan 1994; Davis 1994; DOCIT 1988; Forcht 1994; Pfleeger 1997; Sawicki 1992; Stang and Moon 1993; Tiley 1996).

Networked environments generally have numerous access points, these must be checked and secured (Cairo and Friedberg 1995). The design of the network structure can influence the security of these systems. Networks segmented by intelligent hubs, routers, bridges and gateways make the security of access and traffic more efficient (Baker 1995; Cheswick and Bellovin 1994; Cooper et. al. 1995; Corrigan 1994; Davis 1994; Ernst and Young 1993; Garner 1995; Hughes 1995; Jensen 1994; Pfleeger 1997; Schwartau 1996; Siyan and Hare 1995; Stang and Moon 1994). The effectiveness of these networking tools will depend upon the hardware and software configuration of each within the given networked environment. The filtering of packets coming into, and out of, networks is commonly achieved by using intelligent routers and gateways as firewalls to monitor and control traffic (Garfinkel and Spafford 1991).

The control of user authentication, user access to files and facilities and user activities can be managed by specialised network authentication systems such as Kerberos and SESAME (Baker 1995; Cheswick and Bellovin 1994; Cooper et. al. 1995; Curry 1992; Garfinkel and Spafford 1991; Purser 1993; Siyan and Hare 1995). Devices attached to a network should also be authenticated with restrictions implemented on types of transactions available and given workstations and servers (Cooper et. al. 1995; Corrigan 1994; DOCIT 1988; Ernst and Young 1993). Network monitoring devices can provide information on user access and activities and can terminate sessions where required.

Powerful network analysing software (commonly known as 'packet sniffers') is designed to monitor traffic on networks (DOCIT 1988), however this type of software is a double-edged sword. These programs are not only useful tools for network managers to monitor communications and indicate problem areas, but also

for unauthorised users to capture logon data and other messages (Anonymous 'Maximum Security' 1995; Skillen 1992).

Packet sniffer programs are freely available on the internet (see Esniff, Sunsniff Nitwit.c and Linux_Sniffer.c at *www.catch22.com*/Twilight.NET/ *phuncnet/hacking/proggies/sniffers/*, EtherDump at *www.irdu.nus.sg/security/ ftpl. html*, Ethload at *www.med.ucalgary.ca:70/1 /ftp/dos/regular*, Gobbler at *www.cse.rmit.edu.au/-rdssc/courses/ds738/watt/other/ gobbler.zip*, Netman at *www.cs.curtin.edu.au/-netman/.*, NetWatch at *www.pulver.com/netwatch*, and Sniffer at *www.pris.bc.ca/tech/fas/sniff.html*.

The control of network communications is necessary to ensure the authenticity, integrity and confidentiality of messages. Security measures recommended for communications include message authentication codes and systems, encryption and secure key management, digital signatures, and the physical protection of communications equipment and housing (Cooper et. al. 1995; DOCIT 1988; Elbra 1992; Ford 1994; Hains 1992; Hough 1991; Pfleeger 1997; Rhee 1994; Ware (1991). Specific security measures relating to modems include using separate incoming and outgoing phone lines, using dial-back modems and encrypted modems, and limiting the knowledge of facilities and lines available on modem connections (Alexander 1996; DOCIT 1988; Farrow 1991; Forcht 1994; Garner 1995; James and Chantler 1993ac; Landreth 1989; Troy 1989)

The security of open systems and internet connections is of particular concern as these systems inherently contain no security features (Anonymous 'Maximum Security' 1997; Cheswick and Bellovin 1994; Cooper et. al. 1995; Farrow 1991; Hughes 1995; James 1994; Nelson 1997; Siponen and Kajava 1998; Siyan and Hare 1995). Well designed authentication systems, firewalls, network security policies and consistent monitoring are therefore recommended.

Other authors and researchers discussing the need for network security measures include Benbow, Masters and Cooper (1986), Bentley, Hinde and Oliphant (1995),

Fitzgerald J (1992), Fitzgerald K. (1992a), Forcht (1994), Lane (1985), Wallich (1994), Weiss (1992a 1992b).

A.16 Personal Computer Security

Personal computers (PC's) provide a powerful tool for processing, storing and manipulating information. Because of their power and portability the PC environment is highly vulnerable. Information is easily accessed, downloaded, changed and destroyed and users need to be cognisant of the risks associated with PC's (Forcht 1994; Pearson 1992; Pfleeger 1997).

Security measures recommended for PC environments encompass those for all computer systems, but specifically include:

- policies covering PC acquisition and usage, including password management, illegal copying of software, backups, responsibility for security of each PC (Alexander 1996; Baker 1995; Moeller 1989; Pearson 1992; Pfleeger 1997)
- physical access restrictions including bolting PC's to desks, restricting access by keycards, PINs etc. (Bhaskar 1993; Cowcher 1992; Fink 1997; Forcht 1994; Moeller 1989; Pfleeger 1997; Stang and Moon 1993)
- protection against power surges and power outages (Corrigan 1994; Pearson 1992)
- logical access control measures including the use of access control software, passwords, smartcards and other biometric and electronic devices (Alexander 1996; Bhaskar 1993; Fink 1997; Forcht 1994; Jackson 1992; Moeller 1989; Pearson 1992; Pfleeger 1997; Stang and Moon 1993; Tiley 1996)
- production and checking of access logs and audit trails (Bhaskar 1993; Fink 1997; Pearson 1992; Moeller 1989; Stang and Moon 1993)
- classification of information and data on PC systems (Bhaskar 1993)
- regular execution of anti-viral software, and use of quarantine PC to check for virus infection on disks (Alexander 1996; Baker 1995; Cohen ,1992; Denning 1990; Fink 1997; Forcht 1994; Pearson 1992; Neumann 1995; Tiley 1996)
- encryption of sensitive data and transmissions (Alexander 1996; Baker 1995; Bhaskar 1993; Forcht 1994; Jackson 1992; Pfleeger 1997; Stang and Moon 1993; Tiley 1996)

- secure erasure by shredding old files, i.e.overwriting information on the FAT and physical storage media (Jackson 1992; Tiley 1996)
- risk analysis and contingency planning (Alexander 1996; Corrigan 1994; Forcht 1994; Moeller 1989; Pfleeger 1997; Stang and Moon 1993; Tiley 1996)
- procedures to backup data and software, store backups securely both on-site and off-site, and test backups regularly (Alexander 1996; Bhaskar 1993; Fink 1997; Forcht 1994; Jackson 1992; Moeller 1989; Pearson 1992; Pfleeger 1997; Tiley 1996)
- conducting PC security awareness training (Alexander 1996; Pearson 1992; Pfleeger 1997)
- use of screen-savers and timeout features (Fink 1997; Pearson 1992; Stang and Moon 1993)
- assigning responsibility for security to a Security Administrator (Pearson 1992)
- restrict access to copy facilities (Forcht 1994; Pearson 1992; Moeller 1989; Pfleeger 1997)
- auditing PC's on a regular basis (Moeller 1989; Pearson 1992; Stern 1993)

A.17 Systems Development Security Measures

A lack of controls within a systems development environment can directly affect the integrity, availability and confidentiality of the data held plus the availability of the system itself. Many organisations make virtually no provision for security within the systems development process (Stanley 1993). Some organisations have formal procedures, which are not followed or accepted, and others rely on informal approaches that depend upon the knowledge and experience of staff members.

Security needs to be recognised and managed during the development process, regardless of the methodology used (Stanley 1993) whether it is an evolutionary or life-cycle approach.

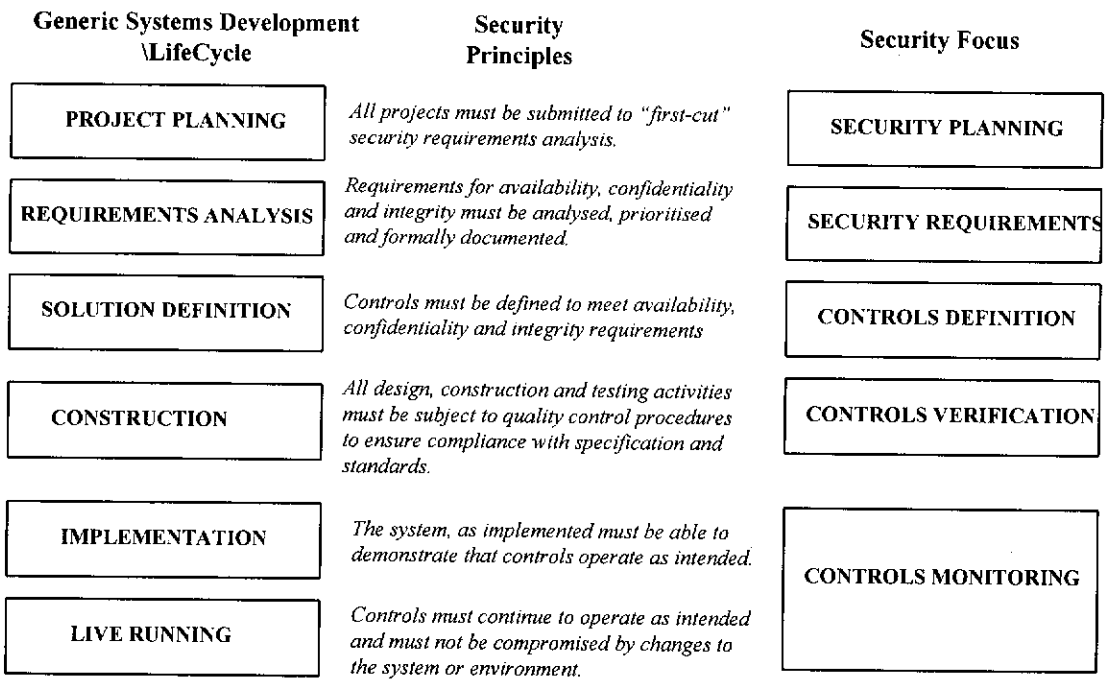

Figure A.5 Security Focus within the Systems Development Life-Cycle (source: Stanley 1993:476)

Figure A.5 illustrates the security principles that apply at each of the generic stages of systems development in order to ensure security features are included in new systems development. This shows the importance of establishing and prioritising security requirements during the systems requirements analysis phase, together with control procedures to ensure specifications are fulfilled during the construction, testing and operations phases.

As the majority of information systems are developed in order to produce information for some level of decision making by management, errors need to be detected early in the development process. Such problems can have far greater impact and are more costly to correct after implementation of a new system (Farrell 1987; Shepperd 1990).

Reasons why IS developments fail, amongst others, include poor project structure, poor project management and control, lack of user involvement, ineffective conversion and implementation planning (Bentley, Hinde and Oliphant 1995). The

information regarding a development project that should be available includes who wrote the code, when, why and on whose authority was it written? What has been written or changed? Who owns it? Who has access to it and who can amend it? (Wilson 1991). The problem of specialisation is particularly apparent in software development environments where software specialists know little about hardware and hardware specialists about software (Abrams and Zelkowitz 1995).

Three major aspects of systems development environments need to be considered with relation to information security; the project management aspect, the composition of the development team (particularly user involvement), and the activities involved in the building of the system.

A.17.1 Project Management

Project management spans all activities in the development process, from the initial planning, through to the ongoing evaluation of operational systems. An important aspect of development project management is a clear definition of the purpose and extent of the proposed undertaking. What is the desired end product? What is the major goal to be achieved? How wide or narrow is the scope? Development projects involve many people of differing knowledge and expertise, and the project manager must be able to articulate well-defined goals (Thomsett 1993; Watne and Turney 1990). If there is a lack of clear goals then superior skills and state-of-the-art equipment will not enable the team to build a successful product. Effective project goals need to be specific, measurable, agreed upon, and realistic and a time frame developed into a project plan (Randolph and Posner 1988).

Project planning ensures the project's objectives are defined and translated into a schedule of work activities. Project control ensures execution of the activities defined in the project plan. The most effective method of controlling a systems development effort is ensuring the project is planned, undertaking ongoing evaluation of the project's progress against predefined scheduled 'deliverables', and revising the project plan where necessary (Ryan 1990). These reviews must include resource allocation and usage (i.e. time, people, equipment, etc.) and the control of quality and adherence to standards.

Additional authors supporting and discussing project management controls include Benbow, Masters and Cooper (1986), Bentley, Hinde and Oliphant (1995), Boom (1990), Fink (1997), Hain (1992), Sapienza (1995b).

A.17.2 User Involvement in the Development

Much literature has been written on the area of user involvement in the systems development process. This is based on the argument that the main objective of computerised systems was to assist employees achieve the objectives of the organisation. Systems were built for users, however, technical people were building the systems with the emphasis on technical specifications rather than an understanding of the human activity involved in making the system work. The involvement of users in the development of information systems has arisen from the organisational behaviour principle of user participation in decision-making (Ives and Olson 1984). The human and social side of information systems was highlighted by Mumford (1981 1983 1985), and subsequent early research in user participation was undertaken by Hirschheim (1983 1985 1986), Land (1982), Olson (1981) and Olson and Ives (1981), amongst others.

However, traditional methods of information systems development incorporating life cycle approaches characterised by limited user involvement have been held to be unsuccessful (Bjorn-Anderson 1983; Bostrom and Heinen 1977; DeMaio 1980; Er 1986; Fitzgerald, Stokes and Wood 1987; Mumford, Land and Hawgood 1978; Vitalari 1983; Yadav et. al.1988; and Yaverbaum 1989). Computer software continued to fail, its developers consistently failing to meet schedules, budgets over-running and the systems failing to meet user and technical performance requirements (Buckley and Poston 1984). The desirable outcomes of the systems development activity; within planned time-frame, within anticipated budget, according to requirements, are rarely achieved, and disastrously costly failures are often the outcome (James and Morien 1991). This has been attributed to ill-defined information requirements, a communications gap between designer and user, and a lack of user involvement in the development process.

In a review of earlier research eight out of twenty-two studies demonstrated a positive relationship between user involvement and various measures of system success, and a further seven present mixed results (Olson and Ives 1981). Overall, however, the generally accepted principle that user involvement is required, necessary, and critical to system success was found by Olson and Ives to be at least exaggerated and at worst incorrect. At best a neutral to slightly positive relationship exists between user participation in systems design and system acceptance and/or satisfaction (Anderson 1985).

System failures have been found to increase in situations where user participation takes place together with severe financial or time constraints. However, increased user involvement has been found to be very helpful in complex projects and almost neutralises its risk (Tait and Vessey 1988). Mature users are able to determine, direct and implement their own information systems and can thus influence both the planning and implementation due to the significance of their understanding of the needs of the business (Dampney et. al. 1984).

A.17.3 Systems Development Project Controls

Controls frequently discussed in systems development project security include the use of a recognised development methodology, establishing written requirements or specifications, designing security measures within the systems design itself, undertaking regular walkthrus as development progresses, performing rigorous testing on the code and the system as a whole, providing systems documentation and separating the development environment from operational systems.

A systems ***development methodology*** entails the breaking down of the development process into smaller, measurable tasks. This ensures all tasks are addressed and allows progress to be easily monitored (Watne and Turney 1990). A recognised development methodology provides a structure for the management of the development project as a whole, regardless of whether it is a highly structured life-cycle approach, or an evolutionary method.

In the past IS developments have predominantly followed the traditional systems development life cycle approaches. These were considered to be sufficiently controlled as the DP development group was well-trained and experienced, used familiar hardware and software and a sound systems development methodology (Harris 1988). Fast track approaches to systems development where quality is traded off against productivity and costs can result in erroneous decisions. However, controlling costs, and any constraints against productivity, must be traded against the cost to the organisation of not meeting its business goals (Krull 1986). Regardless of the methodology used, a methodology is necessary at all levels particularly where there is automation in systems development (Moignard 1995).

The written ***definition of requirements*** (sometimes also called system requirements) are recommended for a number of reasons. Firstly, to provide a set of guidelines to systems designers and developers to detail the optimal target system, i.e. what the user wants and what the system is required to perform. Secondly, they provide a set of specifications against which the final system can be compared. Thirdly, they should establish a set of criteria for the evaluation of the quality of the completed system. Finally, they also provide an effective model of the system being designed (Baskerville 1988).

As illustrated in Figure A.5, security requirements need to be specified as part of the systems requirements, as a system can only be trusted to be as safe and secure as the functionality designed within that system (Forcht 1994; Stanley 1993).

The act of ***designing controls*** and security measures in the systems development process, as well as controls on the design process itself is essential for the assurance of integrity, availability and confidentiality (Baskerville 1988; Lane 1985; Sapienza 1995a; Smith 1991; Stanley 1993; Warman 1993; Wilson 1991). Controls should be designed into systems based upon user requirements and an analysis of risk (Fink 1997; Kleeman 1991) thus supporting the role of users in the design process. Correct analysis and specification of system security requirements directly affects the systems lifespan (Baskerville 1988).

WalkThrus are regular management, user and development team reviews where parts of the new system are reviewed, or 'walked through' with interested parties. Walkthrus assist in identifying problems, omissions and duplications, and also assist in raising user's familiarity with the new system prior to its installation (Harris 1988; Lane 1985). Walkthrus are particularly valuable in the development of systems requiring high levels of security for this reason (Martin 1992).

Testing of the system provides the final opportunity to identify and fix any problems before the new system is implemented. The testing process should ensure that the system objectives have been fully met, the system performs effectively and efficiently, and that all specified controls are included and operational (Fink 1997; Watne and Turney 1990).

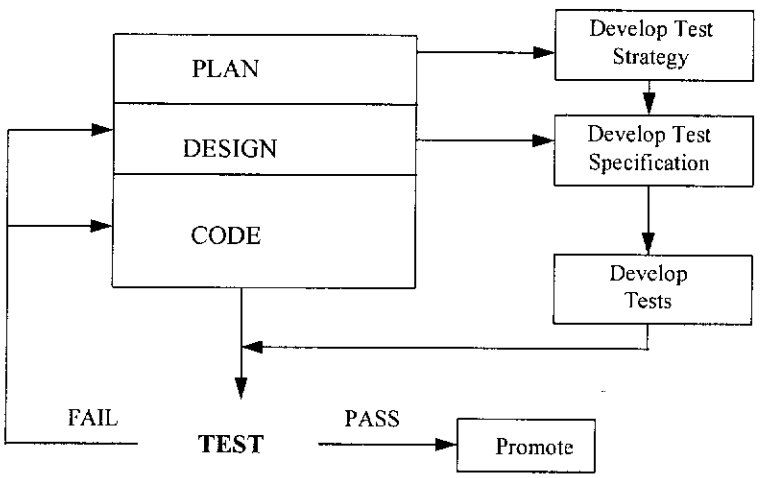

Figure A.6: Systems Development Testing Activities
(source: Lubelski and Kocher 1995:48)

Three stages of testing are recommended; the testing of programs by the development programmers themselves, system testing by the systems analysts to test system functions and integration, and user-acceptance testing by the proposed users of the

system to ensure all requirements have been met (Vasarhelyi and Lin 1988). The testing process should include planning of the test activities, designing of test data and processes and finally the actual testing (see Figure A.6). Where testing is not successful, ie the test fails, then the system may need adjustments to the design, or the test data may require modification to ensure the required specifications are met.

Separate development environments are necessary to ensure live systems are not affected by systems under construction (Bentley, Hinde and Oliphant 1995; Elbra 1992; Wilson 1991; Wood 1982). Strict demarcation must exist between operational and development software and written procedures should govern the process of software transfer from development to live operating environments (Elbra 1992). Procedures to manage version control of systems under development is an important consideration particularly where development is undertaken in multi-user environments (James and Morien 1991).

APPENDIX B

POTENTIAL SECURITY PROBLEMS

APPENDIX B - POTENTIAL SECURITY PROBLEMS

'Using a shotgun to rob a bank these days lacks style' (Power 1994:26)

The potential security problems listed below are not mutually exclusive. Each of the problems has been included based upon its use in previous surveys or publications relating to security concerns.

B.1 Data Error and Corruption of Data

The problem of data errors and corruption of data is a common one. Organisations rely on data held on computer systems to be accurate and valid, and the risk of compromising data integrity by intentional or unintentional acts needs to be addressed (Baskerville 1988; Ware 1991). Data integrity problems are more widespread and of greater significance than attacks on hardware and software (Pfleeger 1997). Corruption of data can be the result of viruses or other forms of rogue code, human error, software errors, errors in system design, or corrupt backups. Problems associated with data integrity have been included in a number of information security surveys (KPMG 1996, 1998; Seah et. al. 1991).

B.2 Loss of Data

The loss of data is a common occurrence, and where backups held are not current or corrupt, organisations may experience considerable financial loss (Alexander 1996; Ware 1991). Loss of data can occur from virus infection and other rogue code, human errors, software and hardware errors and power outages. In addition, the non-delivery of data, email messages or commands, can result from intentional deletion of data and software in the form of sabotage (Neumann 1995). The UK Audit Commission (1994) highlights the problem of lost data, suggesting the value of the lost information is certain to exceed the cost of replacing the equipment and for some organisations the inability to reconstitute lost data could prove to be the difference between business success or failure.

B.3 High Maintenance and Denial of Service

Hardware and software failure threatens the confidentiality, integrity and accessibility of information and systems (Stang and Moon 1993). This causes a denial of service thus affecting the availability of systems and data. Denial of service is defined as 'a temporary reduction in system performance, a system crash requiring manual restart or a major crash with permanent loss of data' (Gasser 1988:4). Denial of use and availability problems causing high levels of maintenance can also result in serious loss of system survivability. Outages can occur accidentally caused by improper systems design, programming and maintenance, or acts of God. Interference from electronic, radar or other signals may also cause non-availability of systems (Neumann 1995).

Alternatively denial of service can result from malicious action limiting or ceasing system operations or denying access to authorised users. This problem is sometimes linked with sabotage, as systems can be trashed so that data integrity is no longer ensured, or authorised users are denied access to the system. Examples of actions resulting in denial of use include destroying data, executing illegal instructions, making illegal system calls that halt system operations, crash or slow the system, or intercepting and redirecting communications transmissions (Gasser 1988).

Research including levels of denial of service as a security problem includes numerous studies by the Computer Security Institute/FBI (Power 1998, 1999) and Benbow, Masters and Cooper (1986).

B.4 Fraud

Fraud is an exploitation of an information system in an attempt to deceive an organisation or take its resources (Stang and Moon 1993:20). Computer crime surveys continue to report high losses from fraud. Significant studies incorporating computer fraud include annual surveys by the Computer Security Institute/FBI (Power 1998, 1999), fraud reports by Peat Marwick (KPMG 1993, 1996, 1998, 1999), crime studies by the UK Audit Commission (1994, 1998), the Singapore Institute of Management and ACARB (Seah et. al. 1991) Benbow Masters and Cooper (1986) and Kamay and Adams (1990, 1992).

Fraud by insiders remains a major problem and can be difficult to detect, hence the rate of undetected fraud is suspected to be high (Neumann 1995). Perpetrators are frequently from inside the organisation, being in positions of trust and having close familiarisation with the systems (Baskerville 1988).

Opportunities for fraud in computerised environments are dramatically increased over those relating to paper methods (Russell 1994). Most known frauds are detected by audit activities or just by chance, thus supporting the need for controls in and around computer systems (Benbow 1992; Bentley Hinde and Oliphant 1995; Fitzgerald, 1992b). Fraud is perceived by management to be an increasing problem in the future (KPMG 1993, 1996, 1998)

B.5 Logical Access Violation and Espionage

Logical access violations are acts of unauthorised access to restricted data and systems. Logical access violations include hacking and cracking by outsiders, unauthorised logical access by employees and industrial espionage.

Hacking is defined as "the process of accessing computer systems by persons who have no legitimate access to the system" (Hoath and Mulhall 1998:16). Hacking also includes cracking passwords, phone phreaking (using masquerade tones to avoid paying for phone calls) and social engineering (impersonation of employees) (Alexander 1996). The most sinister members of the hacker community have been termed 'Cyberpunks' (Clough and Mungo 1992; Hafner and Markoff 1993).

Hacking is a tool used in industrial espionage, where hackers and ex-cold war spies, who are keen to exploit their talents compete for pay-offs. These industrial spies are hired by organisations or individuals to gather information for use in take-over bids, drug and political manoeuvres, or carry out sabotage on chosen systems (Alexander 1996; Rushkoff 1994). Desperate economic conditions and intelligence structures already in place are contributing factors to the rising rate of industrial espionage (Stern 1993).

Knowledge about competitors is often a prime key to success in today's high technology corporate environment, and information gathering has become a formalised aspect of competitive business. The compromise of confidential information relating to trade secrets, marketing strategies, new product data or other sensitive information can cripple an organisation and assure the success of its competitor (Baskerville 1988).

Newman (1993:17) presents information regarding the Society of Competitor Intelligence Professionals in Europe and the USA, an association of information gatherers. Although many organisations state they have never experienced information loss by espionage, Newman points out that information theft is rarely discovered.

The major security surveys include methods of unauthorised access, including the UK Audit Commission (1994, 1998), the Computer Security Institute/FBI (Power 1998, 1999), Kamay and Adams (1990, 1992), the Singapore Institute of Management and ACARB (Seah et. al. 1991) and Benbow Masters and Cooper (1986).

B.6 Physical Access Violation

Physical access violations include intruders trespassing on restricted premises, unauthorised physical access to computer installations and/or restricted workstations (Baker 1995; Carroll 1987; Fink 1997). Physical access violations include sabotage and abuse to equipment or 'machine slaughter' (Pfleeger 1997), acts of terrorism, and piggybacking or tailgating to gain unauthorised access (Jackson and Hruska, 1992).

Security research studying physical access violations include the UK Audit Commission (1994, 1998); Benbow Masters and Cooper (1986); the Singapore Institute of Management and ACARB (Seah et. al. 1991) and Kamay and Adams (1990, 1992).

B.7 Theft of Hardware, Software and Data

The increased rates of theft of hardware, particularly since the availability of laptop computers, has been reported by numerous security studies, including those by the Computer Security Institute/FBI (Power 1998, 1999) and others (Kamay and Adams 1990, 1992). Theft of software and data has also risen as indicated in reports by the Computer Security Institute/FBI (Power 1998, 1999), the UK Audit Commission (1994, 1998) and the Singapore Institute of Management and ACARB (Seah et. al. 1991).

The theft of data and corporate information should be of major concern to organisations and the need for information classification systems to indicate the most vulnerable information is recommended (Bentley Hinde and Oliphant 1995; CSI Roundtable 1998; Peltier 1998). Industrial espionage (see discussion above) is the major form of theft of information.

B.8 Sabotage

Sabotage is wilful physical or logical damage (Stang and Moon 1993:37) or destruction to information systems hardware, software and/or data. Intentional sabotage to an information system emanates from several major sources: disgruntled employees, vandals, and terrorists (Baskerville 1988; Stang and Moon 1993; Stern 1993). Acts of sabotage usually involved other types of security problems discussed, ie unauthorised physical and logical access, viruses and denial of service.

Major security research studying levels of sabotage includes works by the Computer Security Institute/FBI (Power 1998, 1999), the UK Audit Commission (1994, 1998), Kamay and Adams (1990, 1992), the Singapore Institute of Management and ACARB (Seah et. al. 1991) and Benbow Masters and Cooper (1986).

B.9 Unlicensed Software

The unlicensed copying and use of software has been a particular subject of concern over the past decade, receiving high media coverage. The extent of software piracy has been so high that the Business Software Association of Australia was formed in the late 1980's to investigate non-compliance of software copyright and prepare legal

action against defenders (BSAA 1989). This area overlaps with the theft of software area above. Piracy of software has been a factor included in security studies by the UK Audit Commission (1994, 1998), and the Singapore Institute of Management and ACARB (Seah et. al. 1991).

B.10 Rogue Code / Viruses

A virus is a program or section of code that can infect other programs by replicating itself and modifying code or data stored in memory (Pearson 1992; Pfleeger 1997). A worm is a program or section of code similar to a virus that can reproduce itself across a network to devour all available resources, thus causing the system to malfunction or cease operations. Viruses can cause corruption of boot sector, hard disk partition tables or main memory, alter or lock-up files, crash the system, cause delays and other denials of service (Neumann 1995).

Viruses and worms are only two forms of rogue code that can damage hardware, software and data. Other types of rogue code (or 'cybercritters' according to Alexander 1996) include trojan horses, logic bombs and time bombs (Forcht 1994; Pfleeger 1997; Tiley 1996).

A trojan horse is an unauthorised program or section of program code contained within an authorised program, and this type of code is often used to collect information for intelligence purposes (Anon 1997). Many viruses are hidden as trojans in legitimate host programs (Pearson 1992). Trojans are commonly used to capture password data from login programs giving no visible signs of their existence (Neumann 1995)

Trapdoors and Backdoors are covert entry paths into programs and systems that by-pass security controls. Trapdoors may be intentionally planted during the development, testing or maintenance of programs, or may be discovered from flaws or holes in operating systems and other system software (Martin 1992; Neumann 1995; Pearson 1992). Time and Logic Bombs are sections of code that stay dormant until activated by a given set of conditions, such as a combination of keys or a date from the computer clock (Alexander 1996; Forcht 1994; Martin 1992; Pearson 1992).

Many time and logic bombs include attempts at blackmail and extortion (Neumann 1995). Hacker groups predict more future crime in the form of virus attacks and other forms of infiltrating stored computer files (Metchik 1997).

Major security research studying the occurrence of virus attacks include works by the Computer Security Institute/FBI (Power 1998, 1999), the UK Audit Commission (1994, 1998), Kamay and Adams (1990, 1992), the Singapore Institute of Management and ACARB (Seah et. al. 1991) and Benbow Masters and Cooper (1986).

APPENDIX C

DATA COLLECTION DOCUMENTATION

Appendix C.1: Data Summary Sheet

Organisation Information

Organisation Name (Confidential) _____

Organisation Code _____ Industry Code (1-22) _____

System Description _____

Type of Software Platform (1-3) _____

Span of Impact (1-3) _____

System Sensitivity (1-5) _____

Maturity of Users (1-4) _____

Number of Users (actual figure) _____

Degree of Centralisation (1-5) _____

Comments

_____

_____

_____

Corporate Security Measures (1-5, where 1 = absent, inactive: 5 = implemented and active)

Security Policy _____ Security Manager _____

Security Planning _____ Security Supervision _____

Risk Analysis _____ Security Education _____

Contingency Planning _____ Quality Assurance _____

Comments

_____

_____

_____

_____

Operational Security Measures (1-5, where 1 = absent, inactive: 5 = implemented and active)

User Responsibility	_____	Change Control	_____
Physical Access Controls	_____	Communications Controls	_____
Logical Access Controls	_____	Independent Audits	_____
System Logs & Error Handling	_____	Backup Procedures	_____

Comments

_____

_____

_____

_____

_____

Systems Development Controls (1-5, where 1 = absent, inactive: 5 = implemented and active)

Project Management	_____	Design Controls	_____
User Involvement in Development Team	_____	Walkthroughs	_____
Development Methodology	_____	Testing Procedures	_____
Requirements Specifications	_____	Separate Environments	_____
Systems Documentation	_____		

Comments

_____

_____

_____

_____

Security Problems (1-5, where 1 = no occurrence/ no impact : 5 = high occurrence/ high impact)

Data Error	_____	Physical Access Violation	_____
Data Corruption	_____	Software / Data Theft	_____
Loss of Data	_____	Hardware Theft	_____
Denial of Use	_____	Sabotage	_____
Lack of Documentation	_____	Unlicensed Software	_____
Fraud	_____	Rogue Code	_____
Logical Access Violation	_____		

Comments

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Appendix C.2: Rating Descriptions for Security Measures

CORPORATE SECURITY POLICY

1. No security policy exists.

3. The organisation has a written or semi-formalised policy which is partially supported.

5. The organisation has a formalised policy on security based upon organisational goals or missions, which details objectives and policies regarding information or computer security, responsibility for security and the organisation's resource commitment to security, which is actively supported throughout the organisation.

SECURITY PLANNING

1. No plan for security exists.

3. The organisation has a semi-formalised or written security plan which is partially supported and updated irregularly.

5. The organisation has a formalised security plan which details current levels of security and planned improvements. This plan is linked to organisational goals or missions, as well as corporate policies, and is integrated into the contingency plan. Security planning is updated or undertaken annually.

RISK / THREAT ANALYSIS

1. No risk analysis or information classification is carried out.

3. An infrequent risk analysis is undertaken, but it is not integrated into security planning and contingency planning.

5. The organisation carries out a risk or threat assessment annually and integrates this information with security planning and contingency planning. Information is classified according to its sensitivity and all documents are marked with an information classification.

CONTINGENCY PLANNING

1. No contingency plan exists.

3. A partial contingency plan exists, which is tested irregularly.

5. There exists a formalised contingency plan which covers all aspects of disaster recovery for critical systems and the system under review, the assets including buildings, computer and communications hardware, software, personnel and data. The plan has been tested and is tested at least once a year.

SECURITY MANAGEMENT RESPONSIBILITY

1. No-one has been assigned the responsibility for security.

3. The responsibility for security is assigned to an employee who performs a database administration function, or acts at a similar level.

5. The responsibility for computer security is officially assigned to a staff member at a supervisory or management level. Security is their sole responsibility, and this person is evaluated on their performance in the security area.

ACTIVE SUPERVISION OF SECURITY

1. Security is not actively supervised and error reports and out-of-line situations are not investigated and followed-up.

3. Some error reports and out-of-line situations only are investigated and followed-up. Some prevention methods are implemented.

5. Security in and around computer systems are actively supervised, with error reports and any irregular situations investigated, responsibility for their correction assigned, and checking all corrections are completed and authorised. Means of prevention of recurrence are also implemented and checked.

SECURITY EDUCATION

1. No security education is undertaken within the organisation.

3. An introductory security awareness program is undertaken for either all or a selection of employees.

5. An active program of security education is carried out for all levels of employees within the organisation, and the consistent re-enforcement of this education is carried out (e.g. by the use of posters, security awards and the like)

QUALITY ASSURANCE

1. There are no quality assurance measures currently in effect within the organisation.

3. There is a semi-formalised quality assurance function, with incomplete or inadequate standards.

5. There is a formalised recognition of quality assurance functions in IS within the organisation. There are formalised standards for compliance and verification and validation measures are undertaken. Responsibility for quality assurance is assigned to a senior employee.

DISTRIBUTION OF RESPONSIBILITY FOR SECURITY

1. Information security responsibility has not been distributed to staff members in any form.

3. Staff members have ill-defined or loosely assigned responsibility for information security in their work areas, or information security is the sole responsibility of the IS Department.

5. Responsibility for the security of information is allocated to those staff members who are information authors, custodians or users. All staff members are assigned responsibility for security of information in their own work areas. Responsibilities are detailed in written job descriptions, and staff members are evaluated on their performance in this area as part of regular performance evaluations.

PHYSICAL ACCESS CONTROLS

1. Access to the development area is unrestricted.

3. Access to the development area is restricted but not monitored.

5. Access to the development environment (computer rooms, programming and administrative areas) is restricted to ensure that only authorised staff may move around the centre, particularly the designated sensitive areas. Access is monitored by security guards, supervisors or personalised key-card access devices.

LOGICAL ACCESS CONTROLS

1. The organisation has no logical access restrictions.

3. The organisation utilises passwords and restricts user functions to a limited degree.

5. The organisation utilises software security systems which incorporate User ID's and Passwords for all users, restricted Access Levels for all users, and restricted read, write, delete etc functions via Authorisation Tables or similar for all register users of the system.

SYSTEM LOGS AND ERROR HANDLING

1. No record of user access, transactions processed or errors are produced by the system.

3. The systems produces only limited information regarding transactions, errors and user activities. These are not actively monitored.

5. The system produces audit trails of all transactions processed through the system, and system logs of all user activities, detailing user ID, time, date and action taken. The system has well-defined error handling routines and reporting facilities. These logs are monitored and action taken where required to ensure continued security of the system.

CHANGE CONTROL PROCEDURES

1. No procedures exist for change control.

3. Informal procedures exist for processing change requests and development.

5. Active formalised procedures exist for the initiation, authorisation, prioritisation, development, testing, installation, approval and sign-off of changes.

COMMUNICATIONS AND NETWORK CONTROLS

1. No network or communications controls are in place.

3. Networks and communications lines are partially protected, but not appropriately for the sensitivity of the information held or transmitted.

5. Networks and communications lines are protected by isolation devices and control procedures as required by the sensitivity of the systems under consideration. Encryption is installed and actively used for the transmission of sensitive information. Transmissions and network activities are monitored and irregular activities or performance are investigated and resolved.

INDEPENDENT AUDITS

1. No audit reviews are undertaken.

3. Audit reviews are only undertaken when potential problems arise. Management heeds recommendations made by auditors.

5. The organisation's computer operations are subject to periodic (at least annually) independent review from qualified internal or external EDP auditors to ensure the necessary physical, administrative and system controls are in place. Management heeds recommendations made by auditors.

BACKUP PROCEDURES

1. No formalised procedure exists and backups are performed on an ad-hoc basis.

3. Backups are performed at monthly or less frequent intervals and are stored both on-site and off-site. There is no formalised backup procedure.

5. The existence of a formalised back-up procedure to ensure that all relevant data and program files are copied to backup storage devices and kept in a safe storage site both on-site and off-site (remote from the computer centre). On-site backups are performed at least weekly and off-site backups performed at least monthly.

PROJECT MANAGEMENT

1. No project management functions are undertaken.

3. The project has a semi-formalised project plan with detailed activities, time and resource requirements.

5. The project has a formalised project plan, with detailed activities, time and resource requirements. Milestones and deliverables are well defined, and criteria and measurement methods established for determination of progress over the life of the project.

USER INVOLVEMENT IN DEVELOPMENT TEAM

1. User involvement in the development process in minimal.

3. Users are members of the development team but are involved only in certain phases. Project Manager is not necessarily a user.

5. Users are active, full-time members of the development team at all stages of the systems development process. A user is the Project Manager of the project.

DEVELOPMENT METHODOLOGY

1. No development methodology is employed for development projects.

3. A semi-formalised methodology is used for each development or maintenance project. Training and documentation have not been undertaken.

5. A recognised development methodology is used organisation wide for systems development. Employees are aware of the methodology, have received training in the use of it, and have access to written procedures on the methodology.

REQUIREMENTS DEFINITION PROCEDURES

1. There are no procedures for defining requirements.

3. There are semi-formalised procedures for defining requirements. Users are involved and sign off a written requirements document.

5. There are written procedures for defining requirements, and criteria have been established for the evaluation of the final product against the stated requirements. There are also predefined measurement methods defined for these evaluation criteria. Users are involved in the requirements definition process, and sign off the final requirements document.

NEW SYSTEMS DOCUMENTATION PROCEDURES

1. No standards or procedures for documentation exist.

3. Semi-formalised documentation standards and procedures exist for major projects only.

5. Formalised standards for documentation exist and are complied with for all projects. Written procedures also exist for the production of required documentation.

DESIGN CONTROLS AND CONTROLS IN DESIGN

1. No systems design controls are in place.

3. Informal measures are used, or design controls are only partially in place.

5. Formal measures are in place to ensure input, processing and output controls are incorporated into the system design, security and audit requirements are specified and included in the design. Systems design also incorporates modularisation and encapsulation controls, consistency of system architecture controls, and means to ensure essential functions and data structures.

USER REVIEWS AND WALKTHROUGHS

1. No user reviews or walk-throughs are undertaken until project development is completed.

3. User reviews are only undertaken on some systems, with limited mechanisms for controlling required changes.

5. The organisation follows strict procedures for regular user reviews and walk-throughs of systems under development. Users are actively involved in regular reviews, and procedures control the fixing of areas of concern highlighted by such reviews.

TESTING PROCEDURES

1. No standards or procedures for testing exist.

3. Informal standard and procedures for testing are used.

5. Formalised standards and procedures for testing exist and are complied with. Alpha and beta testing is carried out, and test data is established by both designers and users. All parties sign acceptance of testing phase.

SEPARATE DEVELOPMENT AND PRODUCTION ENVIRONMENTS

1. No procedures control separate development and production environments and development projects are undertaken in the same environment as operational systems. No procedures control the transfer of systems from test into production.

3. No written procedures control separate development environments but good practices are followed. Full testing is not carried out and authorisation is not always received before transfer.

5. The organisation supports separate computerised environments for systems under development and operational systems. Both environments are individually controlled and separate test databases are used in testing. Formalised procedures control the transfer from test to production and authorisation is received from Users, Audit and IS Management before transfer. Systems are signed off by all stakeholders prior to live installation.

Appendix C.3: Rating Descriptions for Security Problems

DATA ERROR

1 = The system is not used due to the incorrect data caused by poor software or human error.

3 = Data errors caused by poor software or human error are a problem but are isolated to a single system.

5 = There is no known data errors caused by poor software or human error.

DATA CORRUPTION

1 = Occurrence of data corruption is frequent, and this corruption effects the integrity of other integrated systems.

3 = Occurrence of data corruption is not frequent, however known cases have had detrimental consequences, or are frequent with little consequence.

5 = Data integrity within the developed system is extremely high evidenced by no known cases of data corruption.

LOSS OF DATA

1 = A major loss of data occurs frequently and other systems are adversely affected.

3 = A minor loss of data has occurred infrequently, or a major loss of data infrequently.

5 = No accidental loss of data has occurred.

DENIAL OF USE and SYSTEM MAINTENANCE

1 = The developed system requires frequent maintenance and work progress is hindered by the system's lack of reliability.

3 = The developed system is fairly reliable, but needs regular maintenance.

5 = The developed system is totally reliable and neither the hardware nor software has required maintenance since production installation.

LACK OF DOCUMENTATION

1 = Little or no documentation has been produced, or that which has been produced is of very poor quality.

3 = Only part of the required documentation has been produced, which is of acceptable quality.

5 = The developed system has full documentation which is of high quality.

FRAUD

1 = The loss caused by fraud has jeopardised the continued operations of the organisation.

3 = Infrequent occurrences of fraud of significant value have been experienced.

5 = There are no known occurrences of fraud using computer systems.

UNAUTHORISED LOGICAL ACCESS

1 = There is frequent unauthorised access to software and data, causing lack of confidence in the system.

3 = Frequent occurrence of unauthorised access to software and data have occurred with no further repercussions.

5 = No known cases of unauthorised access to software and data have occurred.

UNAUTHORISED PHYSICAL ACCESS

1 = There is frequent unauthorised access to equipment causing lack of confidence in the system.

3 = Frequent occurrence of unauthorised access to equipment has occurred with no further repercussions.

5 = No known cases of unauthorised access to equipment has occurred.

DATA AND SOFTWARE THEFT

1 = Major dollar loss from software and data theft, and affected operations of the organisation.

3 = Major or frequent occurrence of software or data theft, but with low dollar loss.

5 = No known occurrence of data theft or software theft.

HARDWARE THEFT

1 = Major dollar loss from software and data theft, and affected operations of the organisation.

3 = Major or frequent occurrence of hardware theft, but with low dollar loss.

5 = No known occurrence of hardware theft.

SABOTAGE

1 = Substantial loss caused by sabotage affecting operations of the system and the organisation.

3 = Frequent cases of minor sabotage to computer facilities.

5 = No known cases of computer hardware or software sabotage.

UNLICENSED SOFTWARE

1 = Major and frequent non-compliance with software copyright.

3 = Minor and frequent non-compliance with software copyright.

5 = There are no known cases of unlicensed software in existence or use.

ROGUE CODE

1 = Occurrence of rogue code is frequent, and this corruption effects the integrity of other integrated systems.

3 = Occurrence of rogue code is not frequent, however known cases have had detrimental consequences, or are frequent with little consequence.

5 = There are no known cases of rogue code in the form of viruses, trojan horses, worms, etc.

Appendix C.4: Additional Organisation Information Considered

VARIABLE	DESCRIPTIONS	
INDUSTRY (Based upon Benbow et al, 1986 study)	1 = Agriculture 2 = Automobile 3 = Australian Govt 4 = Banking, Finance 5 = Building, Construction 6 = Computing, Technology 7 = Conglomerates 8 = Education 9 = Food, Beverage 10 = Manufacturing 11= Health, Medical	12 = Insurance 13 = Mining, Metals 14 = Chemicals, Petroleum 15 = Publishing, Communications 16 = Real Estate 17 = Retail, wholesale 18 = State Government 19 = Statutory Authorities 20 = Textiles, Footwear 21 = Transport 22 = Other

VARIABLE	DESCRIPTION
TYPE of SOFTWARE PLATFORM and DEVELOPMENT	1 = Predominantly 3GL 2 = Predominantly Package, Modified 3 = Predominantly 4GL
SPAN of IMPACT	1 = Immediate Department Only 2 = Numerous Departments 3 = Whole Organisation
SENSITIVITY of data held	1 = Restricted to a Number of Individuals 2 = Restricted to a Department or section 3 = Restricted to a Number of Departments, Sections 4 = Restricted to Organisation 5 = Public Access
MATURITY Based on Gibson & Nolan's Model of IS Maturity (1974)	1 = Initiation - automating obvious functions (applications) 2 = Contagion - expanding into other application areas 3 = Control - implementation of controls in and around IT 4 = Maturity - IT viewed as investment for future
NUMBER of USERS	1 = 10 - 20 users 2 = 21 - 80 users 3 = > 80 users
CENTRALISATION	1 = Totally Centralised hardware, software and data 2 = High centralisation, low decentralisation 3 = 50 / 50 - equally Centralised and Decentralised 4 = High decentralisation, low centralisation 5 = Totally Decentralised hardware, software and data

APPENDIX D

RESULTS OF DATA ANALYSIS

Appendix D.1: ***Significant Relationships with Corporate Security Measures***

Corporate Security Measures	Other Corporate Security Measures	Operational Security Measures	Systems Development Control	Security Problems
Security Policy	Contingency Planning Security Education Security Manager Security Supervision Security Planning Risk Analysis	Backups Change Control Communications Logical Controls Physical Controls System Logs User Responsibility	Design Controls Development Method Separate Environments Project Management Testing Dev Team Composition Walkthru's	Loss of Data
Security Planning	Contingency Planning Security Education Security Manager Security Policy Quality Assurance Risk Analysis Security Supervision	Backups Change Control Logical Controls Physical Controls System Logs User Responsibility	Design Controls Separate Environments Project Management Testing	Sabotage S'W, Data Theft Unlicensed S'W
Risk Analysis	Contingency Planning Security Education Security Manager Security Supervision Security Planning Security Policy Quality Assurance	Backups Change Control Communications Logical Controls Physical Controls System Logs User Responsibility	Design Controls Development Method Separate Environments Project Management Requirements Definition System Documentation Testing Dev Team Composition Walkthru's	Loss of Data Rogue Code
Contingency Planning	Security Policy Security Planning Security Education Security Manager Security Supervision Quality Assurance Risk Analysis	Backups Change Control Comm's Controls Logical Controls Physical Controls System Logs User Responsibility	Design Controls Development Method Separate Environments Project Management Requirements Definition System Documentation Testing Dev Team Composition Walkthru's	Loss of Data
Security Manager	Security Policy Security Planning Contingency Planning Security Education Quality Assurance Risk Analysis Security Supervision	Audits Backups Change Control Comm's Controls Logical Controls Physical Controls System Logs User Responsibility	Design Controls Development Method Separate Environments Project Management Requirements Definition System Documentation Testing Dev Team Composition Walkthru's	Poor Document'n Denial of Use
Supervision of Security	Security Policy Security Planning Risk Analysis Contingency Planning Security Education Security Manager Quality Assurance	Audits Backups Change Control Comm's Controls Logical Controls Physical Controls System Logs User Responsibility	Design Controls Development Method Separate Environments Project Management Requirements Definition System Documentation Testing Dev Team Composition Walkthru's	Loss of Data Data Corruption Data Error Denial of Use Poor Document'n Logical Violations

Corporate Security Measures	Other Corporate Security Measures	Operational Security Measures	Systems Development Control	Security Problems
Security Education	Security Policy Security Planning Risk Analysis Contingency Planning Security Manager Quality Assurance Security Supervision	Backups Change Control Comm's Controls Logical Controls Physical Controls System Logs User Responsibility	Design Controls Development Method Separate Environments Project Management Testing Dev Team Composition Walkthru's	
Quality Assurance	Security Planning Risk Analysis Contingency Planning Security Education Security Manager Security Supervision	Backups Change Control Comm's Controls Logical Controls System Logs User Responsibility	Design Controls Development Method Separate Environments Project Management Requirements Definition System Documentation Testing Dev Team Composition Walkthru's	Data Corruption Fraud Physical Violation Sabotage S'W, Data Theft Unlicensed S'W Rogue Code

Appendix D.2: ***Significant Relationships with Operational Security Measures***

Operational Security Measures	Corporate Security Measures	Other Operational Security Measures	Systems Development Controls	Security Problems
User Responsibility for Security	Security Policy Security Planning Risk Analysis Contingency Planning Security Education Security Manager Security Supervision Quality Assurance	Backups Change Control Comm's Controls Logical Controls Physical Controls System Logs	Design Controls Development Method Separate Environments Project Management Requirements Definition System Documentation Testing Dev Team Composition Walkthru's	H'W Theft S'W, Data Theft
Physical Access Controls	Security Policy Security Planning Risk Analysis Contingency Planning Security Education Security Manager Security Supervision	Audits Backups Change Control Comm's Controls Logical Controls System Logs User Responsibility	Design Controls Development Method Project Management Requirements Definition System Documentation Testing Walkthroughs	Unlicensed S'W
Logical Access Controls	Security Policy Security Planning Risk Analysis Contingency Planning Security Manager Security Supervision Security Education Quality Assurance	User Responsibility Physical Controls System Logs Change Control Comm's Controls Backups	Project Management Dev Team Composition Development Method Requirements Definition System Documentation Design Controls Walkthroughs Testing Separate Environments	Corruption Data Error Loss of Data Denial of Use Logical Violation
System Logs and Error Handling	Security Policy Security Planning Risk Analysis Contingency Planning Security Manager Security Supervision Security Education Quality Assurance	User Responsibility Physical Controls Logical Controls Change Control Comm's Controls Backups	Project Management Dev Team Composition Development Method Requirements Definition System Documentation Design Controls Walkthroughs Testing Separate Environments	Corruption Data Error Loss of Data Denial of Use Logical Violation
Change Control	Security Policy Security Planning Risk Analysis Contingency Planning Security Manager Security Supervision Security Education Quality Assurance	User Responsibility Physical Controls Logical Controls System Logs Comm's Controls Backups	Project Management Dev Team Composition Development Method Requirements Definition System Documentation Design Controls Walkthroughs Testing Separate Environments	Data Corruption Data Error Loss of Data Logical Violation Poor Documentat'n
Communications Controls	Security Policy Risk Analysis Contingency Planning Security Manager Security Supervision Security Education Quality Assurance	User Responsibility Physical Controls Logical Controls System Logs Change Control Backups	Project Management Dev Team Composition Development Method Requirements Definition System Documentation Design Controls Walkthroughs Testing Separate Environments	Data Corruption Data Error Loss of Data Denial of Use Logical Violation Poor Documentat'n

Operational Security Measures	Corporate Security Measures	Other Operational Security Measures	Systems Development Controls	Security Problems
Independent Audits	Security Manager Security Supervision	Physical Controls Backups	Project Management Development Method Requirements Definition System Documentation Design Controls	
Backups	Security Policy Security Planning Risk Analysis Contingency Planning Security Manager Security Supervision Security Education Quality Assurance	User Responsibility Physical Controls Logical Controls System Logs Change Control Comm's Controls Audits	Project Management Dev Team Composition Development Method Requirements Definition System Documentation Design Controls Walkthroughs Testing Separate Environments	Loss of Data Denial of Use Poor Documentat'n

Appendix D.3: Significant Relationships with Systems Development Controls

Systems Development Controls	Corporate Security Measures	Operational Security Measures	Other Systems Development Controls	Security Problems
Project Management	Security Policy Security Planning Risk Analysis Contingency Planning Security Manager Security Supervision Security Education Quality Assurance	User Responsibility Physical Controls Logical Controls System Logs Change Control Comm's Controls Audits Backups	Dev Team Composition Development Method Requirements Definition System Documentation Design Controls Walkthroughs Testing Separate Environments	Data Error Denial of Use Poor Documentat'n
Development Team Composition	Security Policy Risk Analysis Contingency Planning Security Manager Security Supervision Security Education Quality Assurance	User Responsibility Logical Controls System Logs Change Control Comm's Controls Backups	Project Management Development Method Requirements Definition System Documentation Design Controls Walkthroughs Testing Separate Environments	Loss of Data Data Corruption Data Error Denial of Use Poor Documentat'n Logical Violation
Development Methodology	Security Policy Risk Analysis Contingency Planning Security Manager Security Supervision Security Education Quality Assurance	User Responsibility Physical Controls Logical Controls System Logs Change Control Comm's Controls Audits Backups	Project Management Dev Team Composition Requirements Definition System Documentation Design Controls Walkthroughs Testing Separate Environments	Loss of Data Data Corruption Data Error Denial of Use Poor Documentat'n Logical Violation Unlicensed S'W
Requirements Definition	Risk Analysis Contingency Planning Security Manager Security Supervision Quality Assurance	User Responsibility Physical Controls Logical Controls System Logs Change Control Comm's Controls Audits Backups	Project Management Dev Team Composition Development Method System Documentation Design Controls Walkthroughs Testing Separate Environments	Poor Documentat'n H'W Theft S'W, Data Theft Sabotage
System Documentation	Risk Analysis Contingency Planning Security Manager Security Supervision Quality Assurance	User Responsibility Physical Controls Logical Controls System Logs Change Control Comm's Controls Audits Backups	Project Management Dev Team Composition Development Method Requirements Definition Design Controls Walkthroughs Testing Separate Environments	Poor Documentat'n S'W, Data Theft H'W Theft Sabotage

Systems Development Controls	Corporate Security Measures	Operational Security Measures	Other Systems Development Controls	Security Problems
Design Controls	Security Policy Security Planning Risk Analysis Contingency Planning Security Manager Security Supervision Security Education Quality Assurance	User Responsibility Physical Controls Logical Controls System Logs Change Control Comm's Controls Audits Backups	Project Management Dev Team Composition Development Method Requirements Definition System Documentation Walkthroughs Testing Separate Environments	Fraud S'W, Data Theft H'W Theft Sabotage
Walkthroughs	Security Policy Risk Analysis Contingency Planning Security Manager Security Supervision Security Education Quality Assurance	User Responsibility Physical Controls Logical Controls System Logs Change Control Comm's Controls Backups	Project Management Dev Team Composition Development Method Requirements Definition System Documentation Design Controls Testing Separate Environments	Data Corruption Data Error Loss of Data Denial of Use Poor Documentat'n Logical Violation
Testing	Security Policy Security Planning Risk Analysis Contingency Planning Security Manager Security Supervision Security Education Quality Assurance	User Responsibility Physical Controls Logical Controls System Logs Change Control Comm's Controls Backups	Project Management Dev Team Composition Development Method Requirements Definition System Documentation Design Controls Walkthroughs Separate Environments	Poor Documentat'n H'W Theft Sabotage S'W, Data Theft
Separate Environments	Security Policy Security Planning Risk Analysis Contingency Planning Security Manager Security Supervision Security Education Quality Assurance	User Responsibility Logical Controls System Logs Change Control Comm's Controls Backups	Project Management Dev Team Composition Development Method Requirements Definition System Documentation Design Controls Walkthroughs Testing	Loss of Data Poor Documentat'n

Appendix D.4: ***Significant Relationships with Security Problems***

Security Problems	Corporate Security Measures	Operational Security Measures	Systems Development Controls	Other Security Problems
Data Error	Security Supervision	Logical Controls System Logs Change Control Comm's Controls	Project Management Dev Team Composition Development Method Walkthroughs	ALL Problems
Data Corruption	Security Supervision Quality Assurance	Logical Controls System Logs Change Control Comm's Controls	Dev Team Composition Development Method Walkthroughs	ALL Problems
Loss of Data	Security Policy Risk Analysis Contingency Planning Security Supervision	Logical Controls System Logs Change Control Comm's Controls Backups	Dev Team Composition Development Method Walkthroughs Separate Environments	ALL Problems
Denial of Use	Security Manager Security Supervision	Logical Controls System Logs Comm's Controls Backups	Project Management Dev Team Composition Development Method Walkthroughs	ALL Problems
Lack of Documentation	Security Manager Security Supervision	Logical Controls System Logs Change Control Comm's Controls Backups	Project Management Dev Team Composition Development Method Requirements Definition System Documentation Walkthroughs Testing Separate Environments	ALL Problems
Fraud	Quality Assurance	None	Design Controls Separate Environments	ALL Problems
Logical Access Violation	Security Supervision	Logical Controls System Logs Change Control Comm's Controls	Dev Team Composition Development Method Walkthroughs	ALL Problems
Physical Access Violation	Quality Assurance	None	None	ALL Problems
Software, Data Theft	Security Planning Quality Assurance	None	Dev Team Composition Requirements Definition System Documentation Design Controls Testing	ALL Problems
Hardware Theft	Quality Assurance	User Responsibility	Requirements Definition System Documentation Design Controls Testing	ALL Problems

Security Problems	Corporate Security Measures	Operational Security Measures	Systems Development Controls	Other Security Problems
Sabotage	Security Planning Quality Assurance	None	Requirements Definition System Documentation Design Controls Testing	ALL Problems
Unlicensed Software	Security Planning Quality Assurance	Physical Controls	Development Method	ALL Problems
Rogue Code	Risk Analysis Quality Assurance	None	None	ALL Problems

Appendix D.5: Significant Relationships with Organisational Factors

Industry and Other Indicators	Corporate Security Measures	Operational Security Measures	Other Systems Development Controls	Security Problems
Industry Type *One Way ANOVA Test*	Contingency Planning Security Education Security Planning Security Policy Quality Assurance Risk analysis Security Supervision	Audits Physical Controls	Design Controls	Data Corruption Fraud H'W Theft Logical Violation Loss of Data Physical violation Sabotage S'W, Data Theft Unlicensed S'W Rogue Code
Type of Software Platform *One Way ANOVA Test*	Contingency Planning Security Education Security Manager Security Policy Quality Assurance Risk Analysis Security Supervision	Backups Change Control comm's Controls Logical controls Physical Controls system Logs User Responsibility	Design Controls Development Method Separate Environments Project Management Requirements Def'n System Documentation Testing Dev Team composition Walkthroughs	Corruption Data Error Poor Documentat'n Loss of Data Denial of Use
Span of Impact *One Way ANOVA Test*	Security Policy Quality Assurance	Physical Controls		Corruption Data Error Fraud H'W Theft Logical Violation Loss of Data Physical Violation Sabotage S'W, Data Theft Unlicensed S'W Rogue code
Sensitivity of Data Held *Correlation Co-efficients*	Security Planning Quality Assurance	User Responsibility Physical Controls	Design Controls Requirements Definition System Documentation Testing	Data Error Fraud Logical Violation Physical Violation H'W Theft S'W, Data Theft Sabotage Unlicensed S'W Rogue Code
Maturity *One Way ANOVA Test*	Security Manager Quality Assurance Security Supervision	Audits Backups Change Control Logical Controls System Logs	Design controls Development Method Separate Environments Project Management Requirements Def'n System Documentation Testing Dev Team Composition Walkthroughs	Data Error H'W Theft S'W, Data Theft
Maturity (IT Growth) *Correlation Co-efficients*	Security Manager Security Supervision Quality Assurance	User Responsibility Logical Control System Logs Change Control Backups Audits	Project Management Dev Team Composition Development Method Requirements Definition Design Controls System Documentation Testing Walkthroughs Separate Environments	None

Industry and Other Indicators	Corporate Security Measures	Operational Security Measures	Other Systems Development Controls	Security Problems
Centralisation *Correlation Co-efficients*	Risk Analysis Contingency Planning Security Manager Security Supervision Security Education Quality Assurance	User Responsibility Logical Control System Logs Change Control Comm's Controls Backups	Project Management Dev Team Composition Development Method Requirements Definition Design Controls Testing System Documentation Walkthroughs Separate Environments	H'W Theft S'W, Data Theft Sabotage

APPENDIX E

ADAPTATIONS OF SSM IN PRACTICE

APPENDIX E - ADAPTATIONS OF SSM IN PRACTICE

Soft Systems Methodology (Checkland 1981) has been adapted as it has been applied in numerous organisational settings. A number of adaptations of the methodology are discussed below.

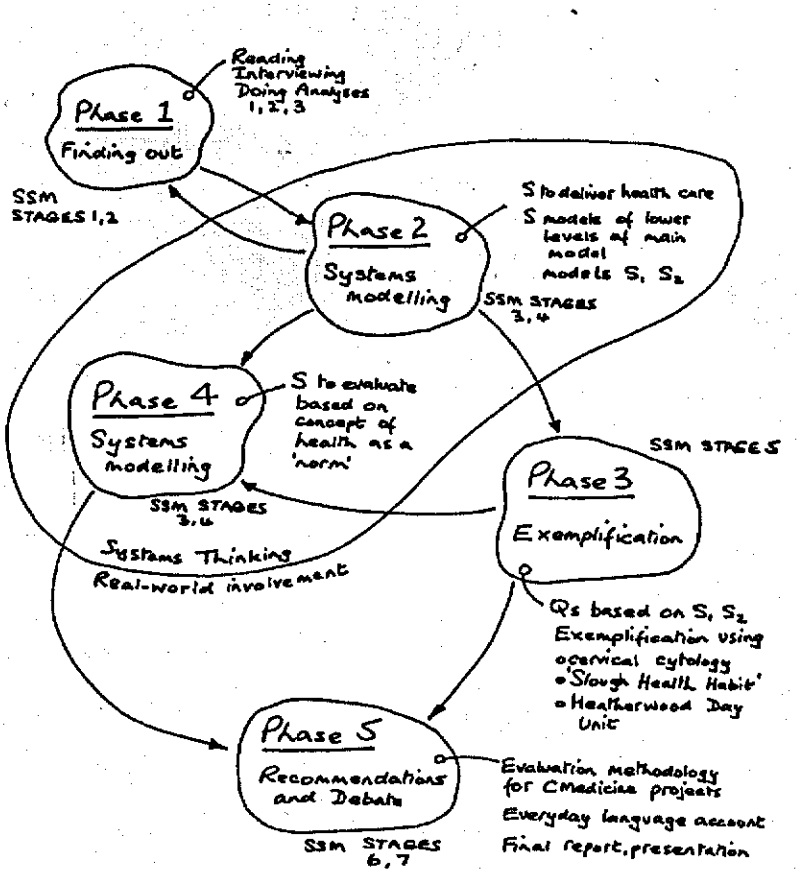

Figure E.1: SSM applied to the East Berkshire District Health Authority

Source: Checkland and Scholes 1990, p102

The first situation is the East Berkshire District Health Authority in the UK for the provision of health care and measuring of its performance. This included

management of resources, policy and political concerns and delivery and management of professional health services. Figure E.1 illustrates the application of SSM to this situation. Note the alignment of SSM stages to phases of the project.

A further application of SSM in the health care industry was undertaken by Elderly Persons Homes, a Social Services Department concerned with managing residential homes for elderly persons. The scope of the project was management of all aspects of residential support plus financial and staff management. This application mapped fairly closely to the original SSM methodology and is illustrated in Figure E.2.

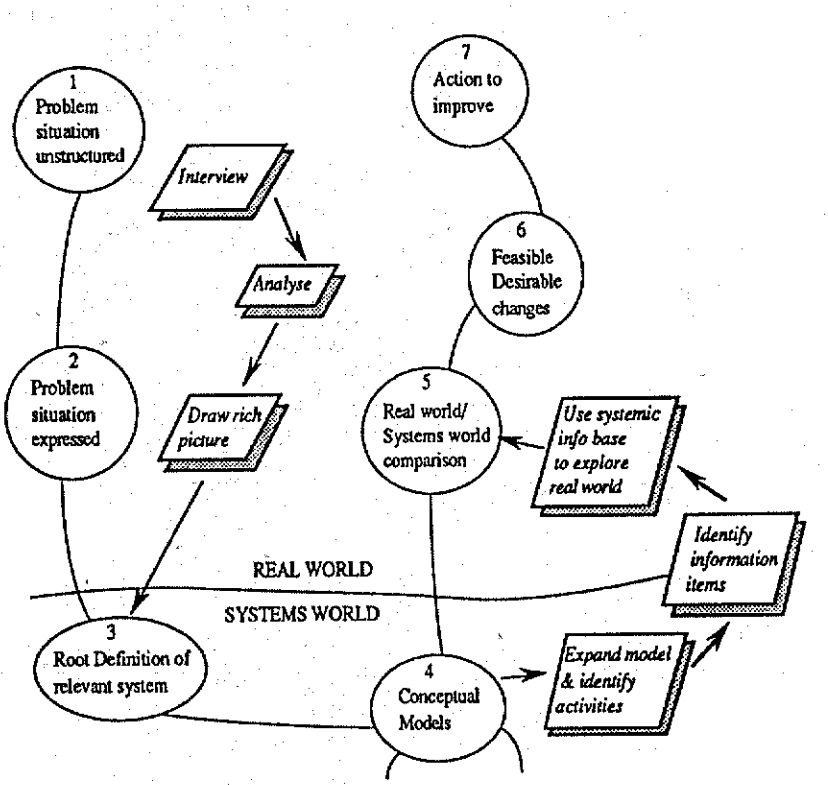

Figure E.2: Elderly Persons Homes Agency Organisational Study

Source: Patching 1990, p169

SSM has been used widely for analysis of engineering functions. The methodology was used to analyse the Central Electricity Generating Board to study the support system managing their operations. SSM was tailored to the situation under consideration, integrating with an adaptive control system modelling approach used by the agency. As can be seen from Figure E.3, more emphasis was placed upon the activities in the systems thinking world in order to analysis the management services role desired for this organisation. MSB in Figure E.3 is an abbreviation for the Board" Management Services Branch, and HAS for human activity system. A similar version of this model was also used for analysing a technical support system in a mining company in Mexico.

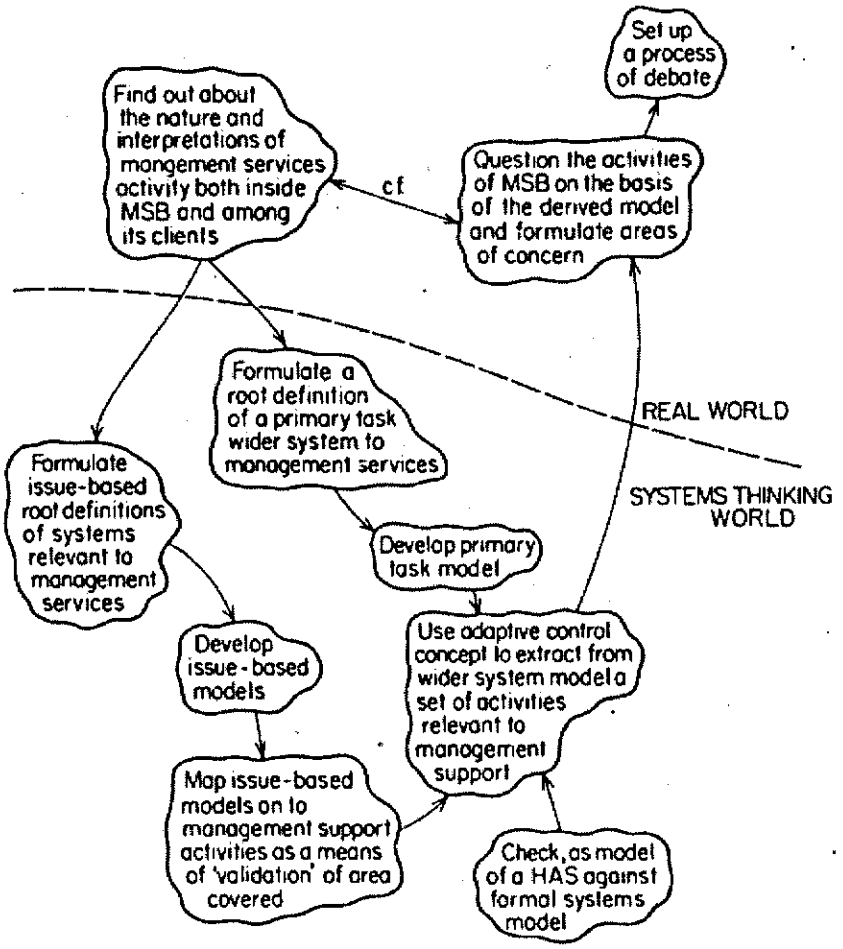

Figure E.3: Management Support System for Central Electricity Generating Board Source: Wilson 1990, p150

Another project utilising SSM as the major analysis method centred upon organisational reorganisation for a Production Engineering organisation in the UK. The adaptation of SSM to the model illustrated in Figure E.4 was considered appropriate by the participating organisation as it satisfied the engineers' need to use a rational approach to restructuring their activities.

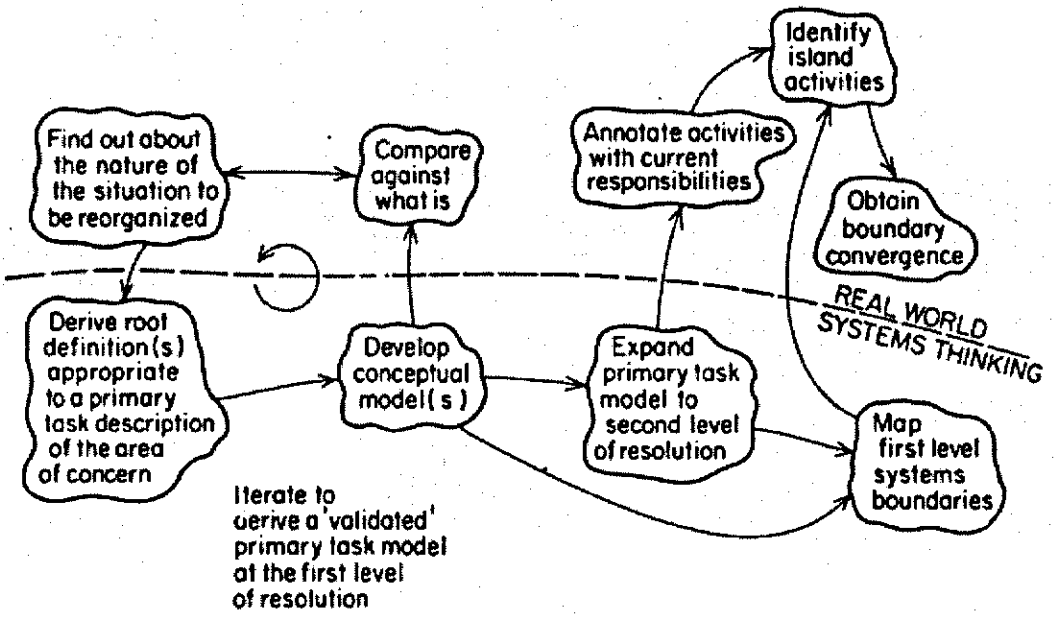

Figure E.4: Production Engineering adaptation of SSM
Source: Wilson 1990, p196

A highly structured application of SSM was undertaken in the Central Computer and Telecommunications Agency to redefine their responsibilities and relationships with other government agencies. This appeared to be a fairly formal study where stakeholders reviewed written documents rather than participating in the planning. A fairly conventional mapping of SSM to the project situation was implemented as illustrated in Figure E.5. However, this version does not differentiate between real world thinking and systems thinking as would normally be seen in an adaptation of SSM.

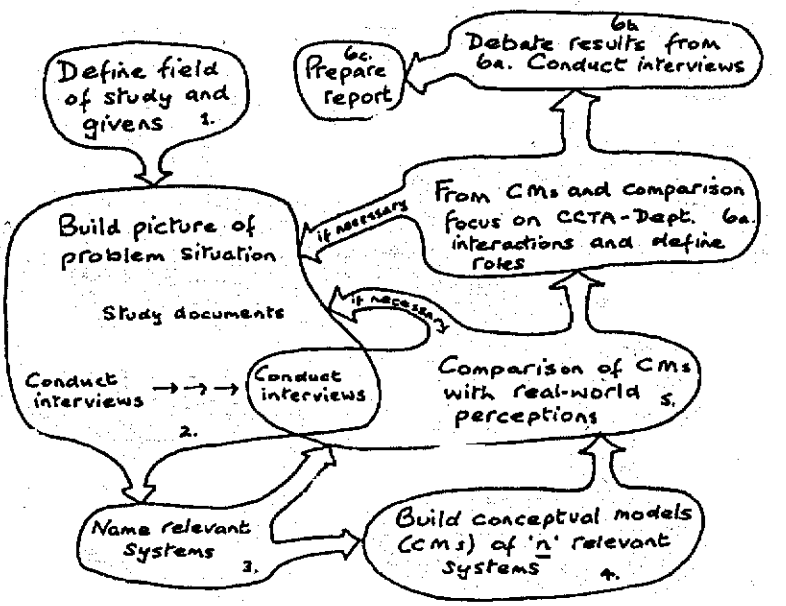

Figure E.5: SSM applied to the Central Computer and Telecommunications Agency Source: Checkland and Scholes 1990, p128

In another project the ICL Corporation used SSM to plan and implement a new organisation culture following a major restructuring of the company. This involved the reviewing and rebuilding of organisational objectives, strategies and tactics. The application of SSM in this situation resulted in a modified approach, consisting of only five major steps. The paradigm shift to and from the real world and the systems world is an integral part of the modified approach. See Figure E.6 for a diagram of the high level approach undertaken at ICL using SSM as a base.

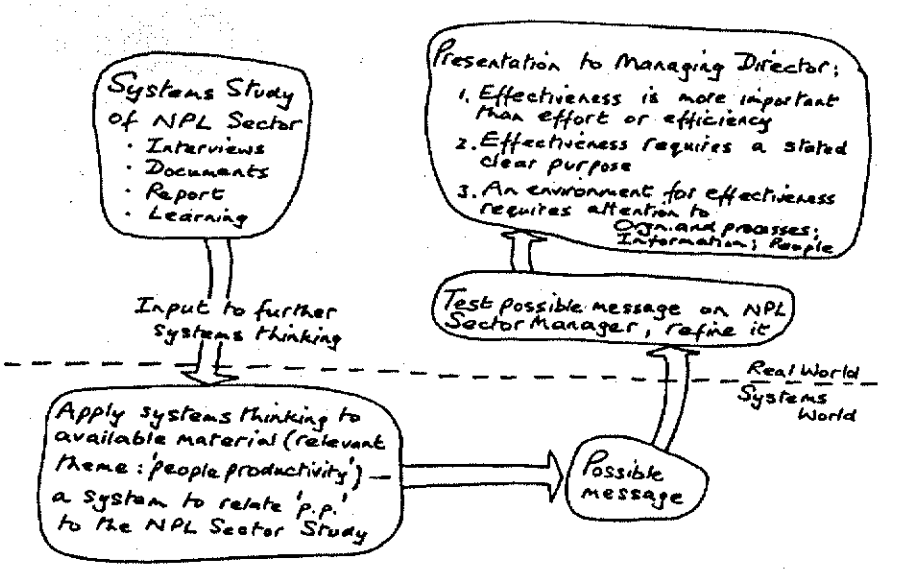

Figure E.6: ICL Strategic Reorganisation Project

Source: Checkland and Scholes 1990, p175

The Product Marketing Division of ICL also used SSM as a base for a redesign of the corporation's Core Head Quarters structure and functions. The approach used specifically for this project required a modification of SSM to take into account the Director's role, however, the first four phases of the Product Marketing Division's application map very closely to the first five stages of Checkland's methodology in theory. Figure E.7 details the approach as it was used in this project.

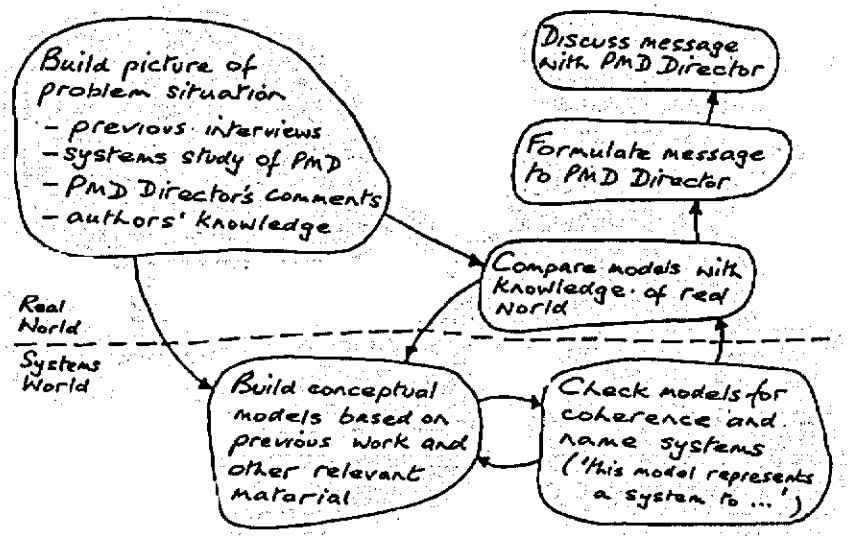

Figure E.7: Product Marketing Division Project

Source: Checkland and Scholes 1990, p208

A tailoring of SSM was commissioned for a bulk and liquid food manufacturing organisation wishing to restructure inefficient computer and manpower resources. This resulted in the adapted approach illustrated in Figure E.8. The approach involved a critical assessment of an existing system of communications, encompassing numerous iterations comparing the information needs derived from primary task analysis with currently provided information systems.

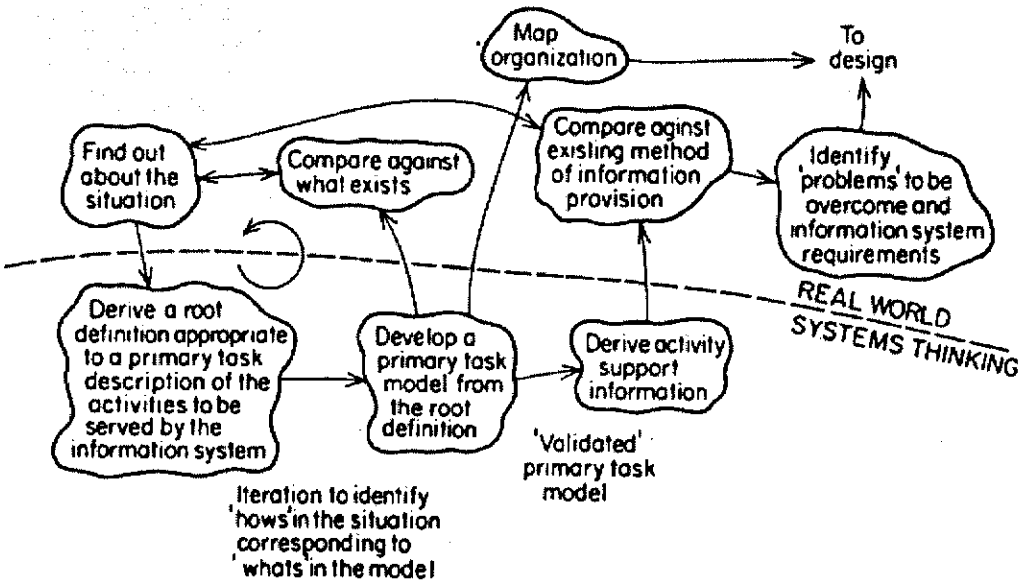

Figure E.8: SSM as adapted for an information systems audit for a Bulk and Liquid Food Manufacturer
Source: Wilson 1990, p215

A reworking of SSM has been presented for a Procedural Audit situation where a conceptual model of a chosen procedure is created and compared with the real situation. Appropriate changes are then determined based upon defined measures of performance. The reworking of SSM to the Procedure Audit is illustrated in Figure E.9.

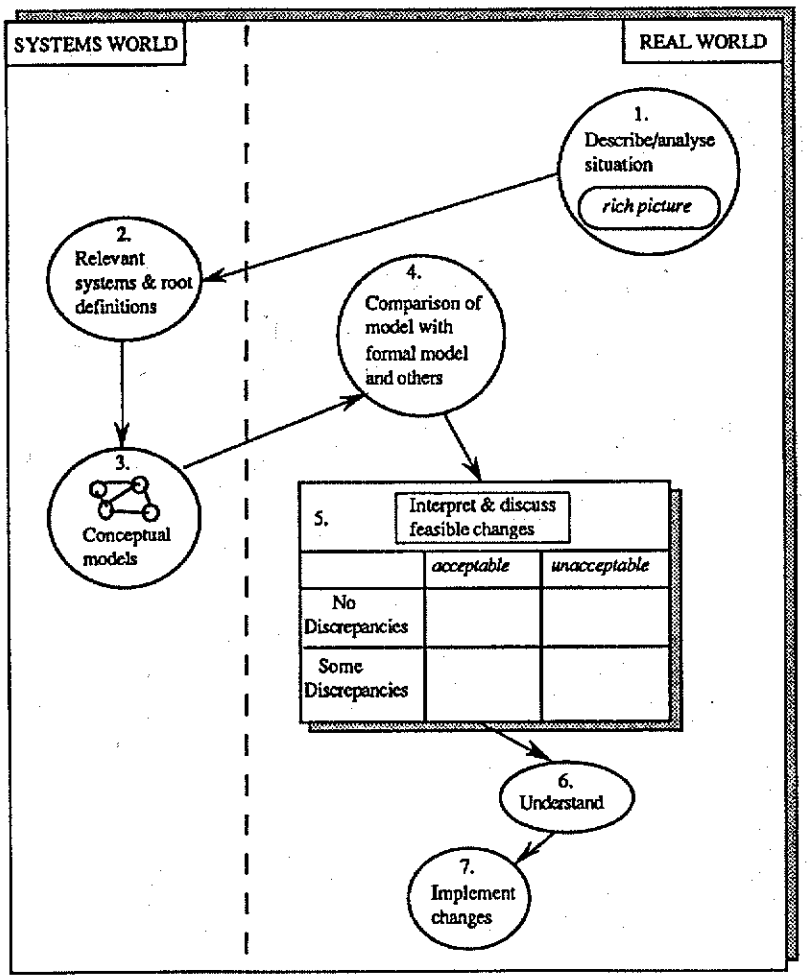

Figure E.9: Procedure Audit System Source: Patching 1990, p218

Many projects have been undertaken aiming to harness SSM for use in the information systems industry. Based upon adaptation of SSM to many different problem analysis situations centred upon information requirements, Wilson (1990) devised the generic model in Figure E.10. This approach aims to derive information needs that are independent of the organisation structure, then relating these to an existing set of management roles. An analysis of information via the use of a matrix termed a Maltese Cross is undertaken in both the systems thinking realm as well as the real world. The Maltese Cross then acts as an extension of SSM for situations involving analysis of information systems requirements.

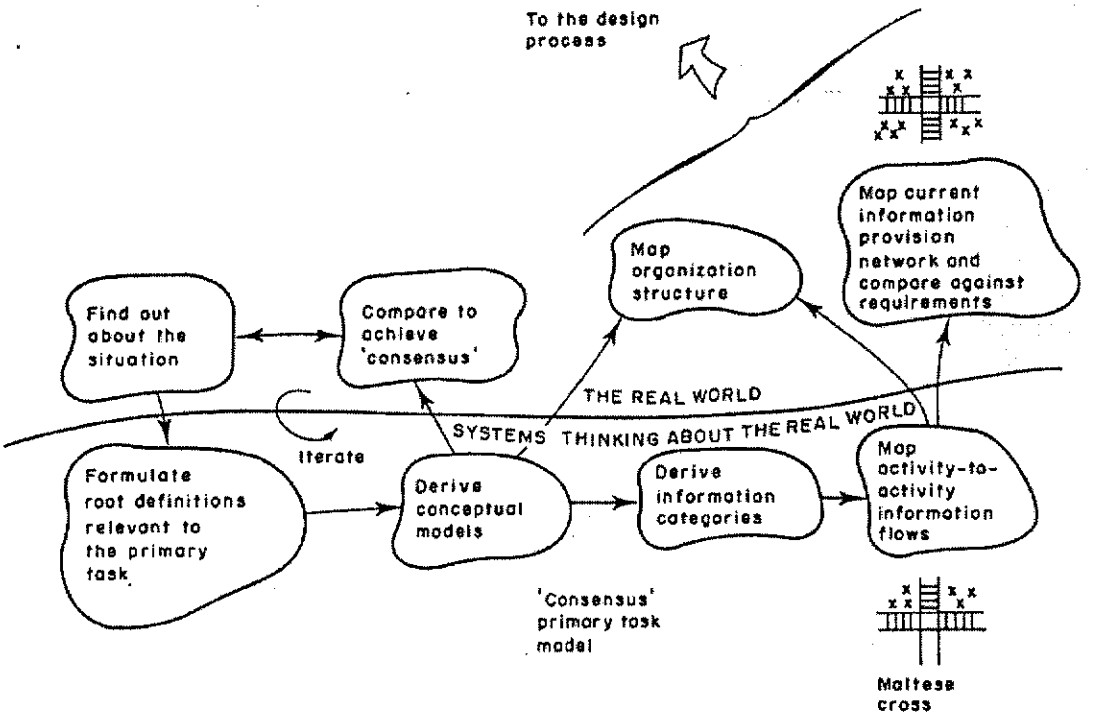

Figure E.10: Information Systems Requirements Model with Maltese Cross
Source: Wilson 1990, p233

APPENDIX F

NAMING THE ORION STRATGEY

It has frequently been said that it is impossible to totally secure computer systems and finding a way of ensuring integrity, confidentiality, availability seems like reaching for the stars. In fact, when reaching for the stars it was found that the Orion Constellation held many parallels with the strategy under development and the Orion Strategy has been named after the Orion Constellation of stars for the following reasons.

F.1 The Orion Formulation

The central star grouping of the Orion Constellation consists of a number of stars in a formation similar to a figure of eight. Figure F.1 illustrates the Orion constellation formation and shows a major group of stars, those of interest to this study being Betelgeuse, Alnitak, Saiph, Rigel, Mintaka, Bellatrix and Meissa.

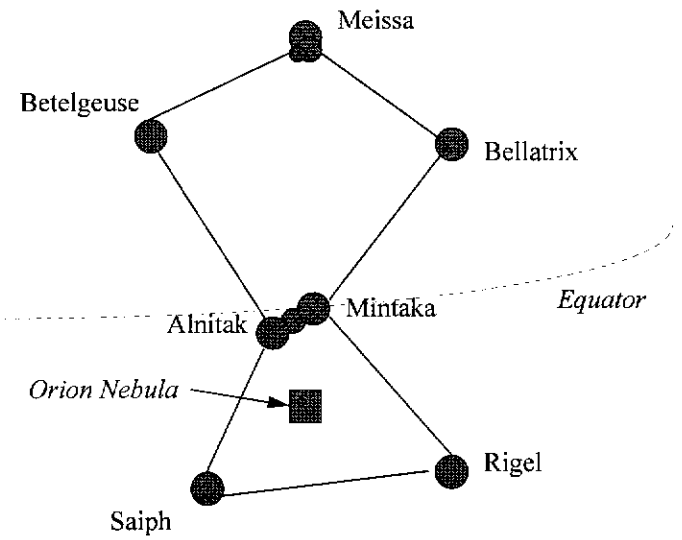

Figure F.1 Constellation of Orion (including Equator)

The positioning of each star and their juxtapositions is of great importance. Comparing the position of each star in Figure F.1 with the activities in the high level model in Figure 6.4, we have a composite picture which looks like Figure F.2 below. Betelgeuse is in a similar position to activity 1, Alnitak to activity 2, Saiph to activity 3, Rigel to activity 4, Mintaka to activity 5, Bellatrix to activity 6 and Meissa to

activity 7. Hence, for each star position there is a related activity in the Orion security management model.

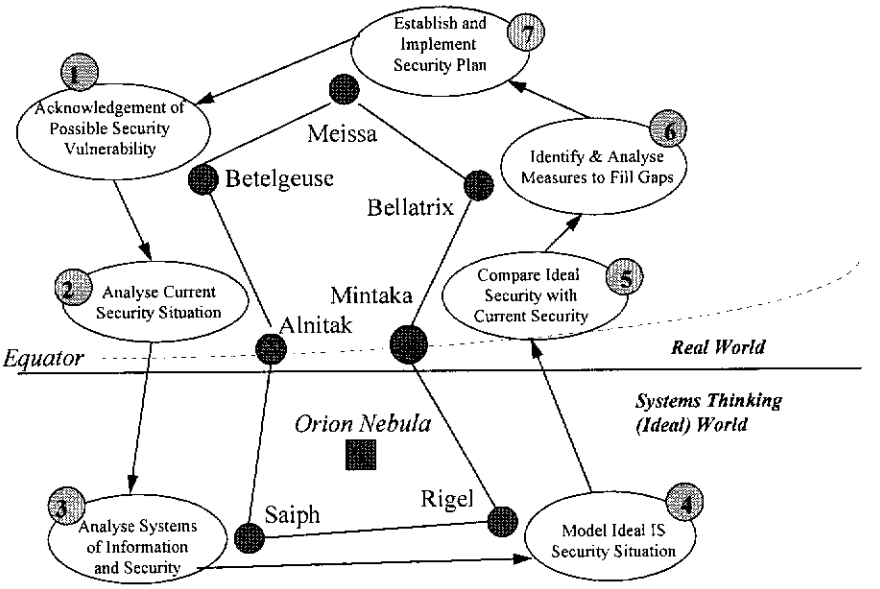

Figure F.2: Comparison of Orion Constellation with Security Activities

F.2 The Celestial Equator

A second important point is that Orion straddles the earth's equator and the celestial equator in December and January, appearing in a Taurus sky. The equator is the imaginary line marking the centre of the earth's surface, dividing the earth into two hemispheres. The equinoctial, or celestial equator, is "a great circle in the heavens corresponding to the plane of the equator when extended" (New Hamlyn Dictionary 1988, p262). As the Orion constellation straddles the equator and celestial equator in December and January, it is visible from both the northern and southern hemispheres, however from the southern hemisphere the formation appears to be upside down. At this time of year the equator is positioned over the three stars, Alnitak, Alnilan and Mintaka, commonly known as the Belt of Orion (see Figure F.1). This is very close to the position of the dividing line between the two hemispheres in SSM and the Orion Strategy, represented by the real world and the

conceptual world(see the equator and dividing line in Figure F.2 above). Just as the Orion constellation is upside down when viewed from the southern hemisphere, so we aim to turn about the perception and thinking patterns of management to encourage creative security solutions in the conceptual world.

F.3 The Taurus Sky

The Taurus sky, ie December and January, is also of significance, as Taurus is the mythical bull, an animal easily initiated into action. The appearance of the Orion constellation in January over the equator signifies a proactive approach, being the beginning of a new calendar year. In security planning and management this equates to planning and action at the beginning of a phase by analysing the situation, being aware of possible risks and their outcomes, and activating protective measures to minimise their effect in advance. This contrasts to a reactive stance where corrective action takes place later in the cycle, for example, after a security violation has occurred.

F.4 Orion - The Hunter

According to Greek mythology Orion is the mythical hunter and his entry into the sky is explained by the following myth. One day Orion was hunting in the forest when a scorpion stung him on the bare heel. He fell to the ground and soon died. But his father, the god Jupiter, brought him back to life again and placed him in the sky together with his two dogs, Canis Minor and Canis Major. There have been other interpretations of the Orion constellation and although the Greeks saw a hunter, other races assigned different meanings to the Orion star formation. According to Reston (1995, p93) the Skidi Pawnee saw deer, the Egyptians saw the god Osiris, and South America's Moche and Chimu people saw a thief thrown to buzzards. Figure F.3 illustrates the formation of the hunter within the Orion Constellation.

Figure F.3: Orion, the Hunter (Supplement to the National Geographic, Dec, 1995).

Orion the hunter is mapped into the star formation as follows (Reston 1995). With the hunter facing us, Betelgeuse forms his right armpit, and six smaller stars outline his club just north of Betelgeuse. Bellatrix the Amazon star, is positioned at Orion's left shoulder; Meissa at his head; and Saiph and Rigel are his right and left knees respectively. Alnitak, Alnilan and Mintaka form Orion's belt from which hangs a sword, consisting of three points of light. A group of stars known as the Orion Nebula, appears at the centre or second point of his scabbard.

Orion's dogs are both positioned on his right, Canis Minor (small dog) situated at shoulder level and Canis Major (large dog) near Orion's right foot (see Figure F.4). Taurus, the bull, can also be seen, where the star Aldebaran sites the bull's eye, the Pleiades group indicate its back, and Menkalinan and Capella are the tips of its two

horns. (See Ellyard 1993, pp 66,72-75 for a more detailed description of Orion hunting the bull with his two dogs.)

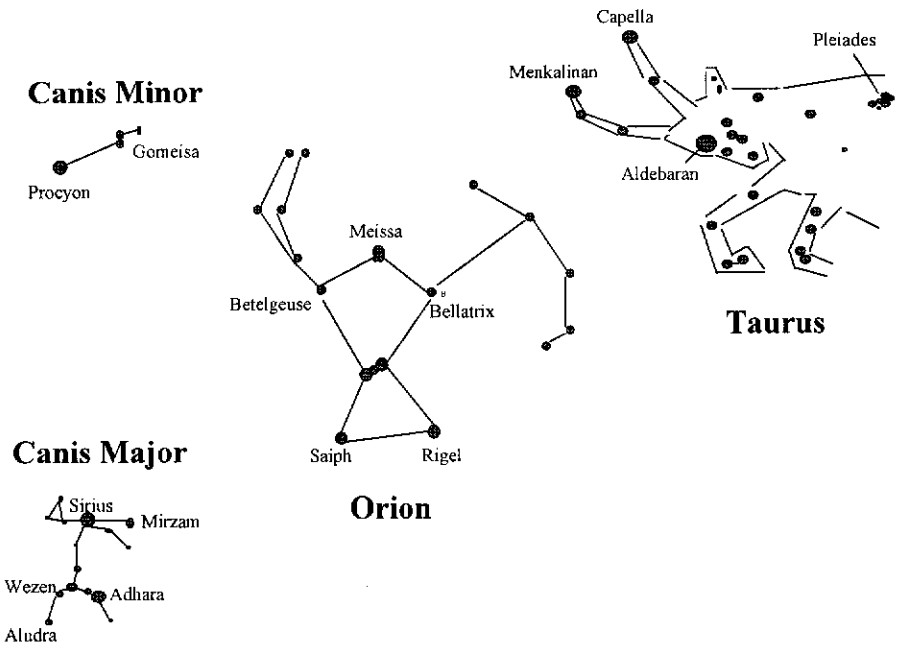

Figure F.4: Orion, with Canis Minor and Canis Major, and Taurus (not to scale)

The hunter principle can be aligned to the management of information security where a group of dedicated staff members work together to search out problems and potential security problem areas within the organisation. The constellation of stars combines to form a powerful cosmic force, much greater than the sum of the individual elements. Similarly, the management team formed to handle information security works together towards a common aim, and the combination of their integrated efforts as a coherent group exceeds the sum of their singular achievements.

F.5 Taurus - The Bull

Taurus symbolises the threats to information, and just as the bull is comprised of many separate and distinctly individual stars and constellations (see top right constellation in Figure F.4), so the overall threat scenario to the organisation is a combination of different types of risks. This grouping of risks can form a formidable force, such as a bull, against which the organisation must protect itself. Hence, Orion

is hunting out Taurus the bull, just as the organisation is hunting out security problem areas.

F.6 The Orion Nebula

The Hubble Space Telescope has recently projected detailed images of the Orion Constellation, and the Orion Nebula (M42), situated just below Orion's belt in the centre of his sword (see Figure F.1 above). This nebula is a place where new stars are born and this stellar "nursery" is one of the most active star-birth regions known. The nebula contains very young stars, no older than a million years, surrounded by small clouds of nitrogen, oxygen and hydrogen gas and dust. The radiant energy from the four bright central stars of the nebula known as the Trapezium (born between 300,000 and a million years ago) excites molecules in a huge underlying cloud (Grosvenor et al 1995). The Hubble Space Telescope's observations of this trapezium region "clearly revealed stars still enveloped in placental material". (Parker 1996, p20).

Of great significance here, is the fact that the Orion Nebula is a place of creation, something unique and of great substance. If one aligns M42 (in the centre of Orion's sword) with the planning approach proposed, this creative source is positioned in the centre of the area shown as the conceptual or ideal world. Here the activities rely greatly upon the ingenuity of the participants to view their organisation and information in a different light. This is the place where new ideas are generated to solve the problems and form a new vision and stance for corporate information security.

F.7 The Orion Myth

There is much written about tales regarding the constellations. Orion has been linked with the weaving industry and in Germany the Orion belt stars were called the 'Mowers' or the 'Rake' as its predawn rising in northern countries was specifically aligned with the flax harvest in August. In addition, the Danes, Norwegians and Swedes "stitched the Belt of Orion to a celestial textile industry and called it Frigg's Distaff" (Krupp 1996, p60). Frigg was a goddess and wife of Odin, the high god who ruled the Nordic cosmos as a divine patriarch and together with Odin she parented

the rest of the Norse gods and goddesses. In Nordic tradition power belonged not to the patriarchs but to the Norns, the 3 goddesses of destiny - Urd (Past), Verdandi (Present) and Skuld (Future).

This concept of power being held by other trusted and influential bodies rather than the supreme leader select is projected into the Orion Strategy. The knowledge and expertise (in business activities, organisational functions and politics, etc) of the participating group is a powerful force executive management can harness and direct. This supports the goal of handing the problem back to those who are stakeholders in the problem situation itself. What better group of people could there be to conceptualise and develop solutions to an idiosyncratic (used in its purest sense) situation.

As Malin and Frew (1995, p307) observed, "Orion is especially rich in beautiful double and multiple stars, and nebulosity both bright and dark is found in many regions. There is no global cluster, but several open clusters are known, some of which are brilliant scattered groups". The variety of stars and their characteristics is reflected in the composition of the security planning group, each participant with their own perspectives, talents and creative ability. In the researcher's experience, the best solution to problems more often than not is found by looking within.

APPENDIX G - COMMENTS FROM THE QUESTIONNAIRES

Security Policy

"The development of a security policy is the highest priority. It should form part of an overall information policy, incorporating a classification of information and access policy."

"A policy restates, clarifies, compliments and reminds all staff of their obligations to promote security within the hospital."

"A security policy needs to be clear and plain and needs to be signed off as an indication that it has been read and understood."

"The security policy needs to cover all personnel, including Doctors. Cleaners also need to be aware."

"The security policy needs to be more specific and detailed."

APPENDIX H

HOSPITAL MISSION AND GOALS

APPENDIX H - HOSPITAL MISSION AND GOALS

VISION - Leading the way in health care provision

MISSION - To provide high quality health care as a unique private teaching hospital

MOTTO - Caring for you is our commitment

CORE VALUES

- Respect for the individual
- Teamwork
- Pursuit of excellence
- The Hollywood spirit
- Contribution to the community

OUR GOALS

1. **New Private Transformation**

   To be recognised by doctors, patients, families and the local community for giving better care and service than any other private hospital.

2. **Revolutionary Management**

   To create a working environment where people achieve and feel valued.

3. **Industry Flagship**

   To create a unique private teaching hospital environment that results in local, national and international recognition for excellence.

* * * * * * * *