Hosie, P. & Smith, C. (2004). Preparing for Crises with Online Security Management Education, *Research and Practice in Human Resource Management*, 12(2), 90-127.

Preparing for Crises with Online Security Management Education

Peter J Hosie & Clifton L Smith

Abstract

Rising incidences of global terrorism and major criminal activities have underscored the need for high quality professional education in security risk and security technology as components of crisis management. This demand for human resource development about security management is reflected by a professional security education course developed by a Western Australian university. Learning materials developed for this course have unique attributes which include constructivist learning principles designed to provide realistic simulations and interactivity. A unit in physical security is featured to illustrate the learning processes and interactive activities incorporated into the development of these online interactive activities. Implications for HRM adopting Technologically Mediated Learning to prepare for crisis management in South East Asian communities are discussed.

INTRODUCTION

Global terrorist events and international criminal acts have considerably increased the demand for high quality education about security management (Caudron 2002). Terrorist tragedies and serious criminal activities in the international context of Kenya in 2001, New York and Washington (9/11) in 2001, Bali in 2002, Morocco, Saudi Arabia in 2003/4, Iraq in 2003/4, and in Indonesia during 2004 have demonstrated the need for high impact professional education for the protection of people and facilities. The need to manage crises from terrorist attack on persons and facilities, in the national and international domain, has never been greater in the international community. These events have focused national and international attention on the necessity for the professional education of personnel in security technology, security management, and security risk for government for private organisations, and community services (Smith 2001, 2002a, Caudron 2002). Consequently, organisations now require high quality security and risk education programs. Terrorist attacks are considered a civil crime, and as a result are under the jurisdiction of police services, which may involve military intervention. Thus, the demand for security education courses for the protection of people and assets is high in the national and international contexts.

Many institutions are offering online education in crisis management. One of these institutions is a Western Australian university, Edith Cowan University (ECU) that has been providing professional security management education in international and national domains since 1993. The introduction of this program coincides with the onset of the suspected al-Qaeda terrorist acts detailed in Appendix 1. Across the wider domain of education, there has been a considerable increase in applications for enrolment in security courses since 9/11, as evidenced by the worldwide availability of online university crisis management courses (Smith 2002a). Consequently, learners are enrolled in the Graduate Certificate in Security Management course in all five major continents. The course has been established on the themes of security technology, security risk, and security management. It has been designed for both distance and online delivery and has developed a reputation for providing excellent learning experiences for participants (Smith 2002a). The course in security management is now widely recognised as a high quality educational program in the national and international contexts by both government and industry (Hesse & Smith 2001).

This paper shows how learning experiences are achieved by integrating crisis management concepts and practices to support the Crisis Management Model shown in Figure 1. A unit in physical security is featured to illustrate the online learning processes that have been incorporated into this course. This learning is situated within the context of the crisis management literature. The philosophy and pedagogy informing the design and development of security management online units are illustrated with examples of interactive simulations and graphics for crisis management for the unit in physical security. Lastly, implications are discussed for HRM using Technologically Mediated Learning (Hosie 1993, 1994) to prepare for crisis management in the South East (SE) Asian region.

CRISIS MANAGEMENT

According to Mitroff (2004), crisis leadership principles should be promoted by HRM professionals as a key aspect of crisis management. HRM professionals have a critical role to play in assessing the corporate culture, and in particular how much denial there is about the need for crisis management education at all levels of an organisation. In Mitroff's view there is potential for HRM professionals to take a more active role in crisis management, provided that they understand the phenomena and are motivated to take on this role. Mitroff (interview cited in Creelman 2004) is reported as saying:

> There are generally two kinds of organizations. Ten to fifteen per cent are proactive and the rest are reactive. Reactive organizations only prepare for a crisis after it has happened. Proactive organizations prepare for crises before they happen ... This is a very important difference. We've found that the proactive organizations have, over the last three decades, experienced, on average, 22 major crises, whereas the reactive ones have suffered from 33. The average return on assets for the proactive firms was six per cent and for the reactive just two per cent. We cannot determine cause and effect, but we do know that there is something very different going on in the proactive organizations.

Mitroff (2004) believes that to become proactive in crisis management it is necessary to change an entire organisation's corporate culture. Proactive companies, it is argued, have a tendency to follow the principle of not harming any individual to guide their conduct. In contrast, reactive corporations, do what is right, but only if it is cost effective. Ironically, Mitroff (2004) argued that reactive companies, whose foremost concern is making money, without regard for individual well-being, invariably end up being less profitable. Resources invested in HRM initiatives to change corporate culture related to crisis management ultimately pay off from both an ethical and business perspective.

Crisis Management Model

Crisis management has developed as a response to natural disasters (e.g., floods, fire, famine, earth quakes) and mismanagement (e.g., Three Mile Island, Chernobyl, Exon Valdez). Approaches to, and the structures associated with, crisis management have evolved from militarist responses to warfare and natural disasters. Contemporary conceptualisations of crisis management deal with broader issues of prevention and mitigation, as well as the need to deal with issues related to response and recovery (Heck 1991, Rosental & Pijnenberg 1991). Terrorist acts during the early years of the 21st century have focused attention on how to manage crises. Corporate initiatives to learn from these events has stemmed from the realisation that crisis management needs to prepare for terrorist acts. An important part of these 'systems and activities' involves the education of key personnel. An organisation's capacity to respond to a crisis can have a significant impact on its short and long-term survival. Implicit in preparing for extraordinary events is the realisation that organisations need to be prepared for crises that are yet to be experienced.

As Heath (1993) observed, many Western organisations concerned with crisis management have invariably adopted a four-stage model, such as the MPRR (mitigation, preparation, response, recovery), or the PPRR (prevention, preparation, response, recovery) as shown in Figure 1. Both the MPRR and PPRR are iterative models intended to provide ongoing opportunities for learning. Education about crisis management relates closely to the 'preparation' aspect of both the MPRR and the PPRR models. The prevention, preparation, response, recovery aspects of the model depicts a flow of events. The sequence logically begins with the 'preparation' phase, but as stochastic events like 9/11 have shown it may actually begin with a 'response', when the 'preparation phase' is inadequate. As such, the 'preparation', 'response', and 'recovery' elements of the Crisis Management Model are interrelated, and, therefore, have a crucial relationship to the 'learning' purpose. Learning is, therefore, an axiomatic and critical recurrent feature of the Crisis Management Model.

Figure 1
Crisis Management Model

The PPRR aspects of the Crisis Management Model can be applied to local facilities and organisations, national infrastructure such as electrical power distributors, and national government organisations such as the military and police services. The role of learning in crisis management is crucial as it is provides the means through which organisational processes and outcomes can be achieved (Smith 2001). In order to achieve a more professional approach to crisis management, organisations need to effectively prepare, plan, and implement especially for security and natural disaster threats, by assessing the risk to the organisation and evaluating the consequence of a terrorist event occurring. Iterative learning is the central focus of the Crisis Management Model in this process.

Lessons Learned from September 11, 2001

Although we owe a great debt to those who responded, perhaps our greatest obligation is to learn from the past so that even better preparation will exist in the future (O'Connell in Smith 2002). 'Preparation' was identified as the main element of the Crisis Management Model requiring attention to ensure learning post 9/11. An overview of key lessons learned from 9/11 is given in Appendix 2 by PriceWaterhouse Coopers (2001). From the 9/11 tragedy, it was clear that those involved were completely unprepared for the events on that day. These recommendations would be an important part of any crisis management plan. HRM professionals would be well advised to take particular note of the general call to increase knowledge and the particular recommendations for testing and training. Failure to properly integrate learning with management processes, as was evident with the 9/11 tragedy, has high potential for entirely inadequate responses to be made to major crises. This discussion of a university course in security management, as applied to crisis management, provides an example of the preparation phase of crisis management. An online aspect of a unit of study in physical security is featured to demonstrate the efficacy of using online learning as part of management mission to prevent loss of control before a crisis.

NATIONAL INCIDENT MANAGEMENT SYSTEM (NIMS)

Prior to 9/11, it was difficult to get people to think about terrorism even though 80 per cent of terrorist acts happen to businesses (Mitroff cited in Creelman 2004). Following the 9/11 crisis the US Department of Homeland Security has developed the first national, standardised incident management approach to emergency incidents, known as NIMS (Brown 2004). This recently adopted management approach builds on the established and successful incident command system derived from the experience gained from 9/11 and elsewhere. NIMS is an expression of the awareness of the changed circumstances facing those who respond to emergencies. NIMS establishes standard incident management processes, protocols and procedures so that all personnel, at all levels of government can coordinate their response actions. Standardised procedures ensure that responders share a common focus and are be able to place full emphasis on the crisis at hand. NIMS ensures that everyone responding to an emergency event uses the same management approach in order to communicate using standard terminology to resolve the incident as quickly and efficiently as possible. Clearly, NIMS is a major initiative in crisis management.

The Security Market

Communities and individuals have always used physical security methods to protect their valuables, a trend that continues in this era. However, as the tools and devices available to criminal and terrorist elements become more sophisticated, law enforcement agencies and security professionals need to have a comprehensive knowledge and understanding of the threats, risks, and security principles necessary to protect a corporation's and society's infrastructure. As the amount of crime and terrorism continues to increase, and it impacts on the community in financial and social terms, so does the need for better strategies for protecting assets (Smith & Robinson 1999). In addition, organisational components of commercial, retail, and industrial organisations as well as leisure facilities all require a security management plan to protect the assets of employees and visitors, the managerial and financial

information of the facility, and the material contents of the organisation. Consequently, worldwide demand for high quality professional education in security issues has emerged commensurate with the international escalation of terrorism (Hesse & Smith 2001).

The market for the security management education courses is extensive within Australia and in the international context such as in the United Kingdom, Europe, the USA and SE Asia (Caudron 2004). National and international demand for professional security managers and consultants is rapidly increasing. For instance, the growth and recognition of academic security programs in SE Asia have only been established over the last decade. This occurrence reflects the rapid growth of the security industry and the demand for security services and products by business, industry and the broader community. ECU's security management learning program is one of a very small number of high quality security courses in the international context that is informed by the Crisis Management Model.

This security management course is recognised to have high status through its acceptance by government agencies, intelligence, police and military agencies, professional employers, and current graduates and learners. The strengths of the educational program are the major emphases on security risk, security technology, and security management as components applied to the Crisis Management Model that provide a comprehensive professional learning experience for government, commercial and industrial security management as well as for security and crisis consultancies. Courses on these themes have been presented for organisations with established anti-terrorism programs, such as in Singapore and Malaysia. Thus, effective security education has become increasingly important to industry and governments in SE Asia because of the moral and legal responsibility of a company to ensure that employees have appropriate education and training to carry out their work safely, to avoid compensation and risk liabilities, and the need to achieve a competitive advantage through increased productivity (Hosie 1993, 1994).

THE ECU SECURITY MANAGEMENT COURSE

The units of study in the Graduate Certificate in the Security Management course provides an emphasis on best practice through reducing the risk of personnel and asset loss from high threat situations to combat criminal and terrorist threats. The units of study in the course comprise:

Physical Security: Principles and applications of technology used in physical security systems, such as: safes, perimeter protection, structural strength of buildings, vehicle control and physical barriers.

Security and Risk Management: Security risk management concepts, and the application of criminological theory to security, including an introduction to risk theory and the analysis and management of security risk.

Intrusion Detection Systems: Security technologies and devices for barrier detection, open ground detection, and intruder detection systems, including microphonic, PIR, microwave and ultrasonic detectors.

Facility Management 1: Interaction between fire and technology management of large facilities including detection systems, alarm systems, high-rise fire management, energy management and light control.

The four units of study have been developed into online learning resources that emphasis the application of professional best practice through reducing the risk of asset loss such as regional and national infrastructure from high threat situations. These outcomes are achieved through the use of constructivist approaches to online learning practices (Steffe & Gale 1995). The development of online security units has been well received by the international security industry. Consequently, information technology has been employed as a potential source of competitive advantage for delivering courses internationally in the learning industry (Hosie, Mazzarol & Jacobs 1998). Conducting a learning needs analysis is an established starting point for the instructional design process.

Learning Needs Analysis

The Graduate Certificate in Security Management course has been structured to meet industry and government requirements. The course seeks to provide the specific and generic content as well as the skills and the knowledge necessary, (i.e., 'Graduate Attributes') for the protection of the assets of organisations and individuals through appropriate learning activities. Aspects of the PPRR model are integrated with the course conceptualisation and delivery to mode to ensure a constant reinforcement of the content and principles underlying the Graduate Certificate in the Security Management course. The course provides the principles underlying the protection of the assets of an organisation, and encourages the learner to seek examples and applications of the security practices in the community, such as public facilities and community assets. Crisis management is an important aspect of this course, but rather than being included as a stand-alone feature of the course it is integrated with the units to ensure that the PPRR components are constantly revisited in various contexts.

An iterative, constructivist learning process is incorporated into the PPRR conception of crisis management, using

the principle of 'double loop learning' (Argyris & Schön 1974, Argyris 1993). The emphasis of double loop learning is on complex and unstructured problem solving which changes as the problem solving capabilities of the learner advance. Planning, implementation, and review are part of the double loop learning process, which complement the PPRR model of crisis management. Ongoing learning is integral to the Crisis Management Model, with the central focus on 'preparation' for the protection of assets in international and national arenas. Essentially, this course in security management is designed to orchestrate learning - the central focus of the PPRR model of crises management on the central themes of security technology, security management, and security risk.

Instructional Design Considerations

Flexible learning technologies have been embraced in the development of the online Graduate Certificate in Security Management course to orchestrate quality course delivery across boundaries at low cost. Well-conceived and implemented use of technology is a means by which learning can be made more flexible and supportive of the principles of adult learning (Hosie 1993). Courseware incorporating Technologically Mediated Learning needs to be professionally designed and evaluated, effective learning strategies adopted, and self-directed learning encouraged (Mazzarol & Hosie 1997).

This design primarily adopted an exogenous constructivism (Moshman 1982) approach which recognises the role of direct instruction, but emphases learners directly constructing knowledge representations (Dalgarno 1996). Elements of endogenous constructivism (Moshman, 1986) were also incorporated into the design in the form of simulations that allowed the learner to explore aspects of the security world first hand (Dalgarno, 1996). For example, the Defence in Depth principle simulation (Figure 4) requires learners to develop their own physical, psychological and procedural methods to deter attacks on a facility. Matching and grouping of symbols allows the learner to get feedback on their knowledge constructs. Another example is the Security Lighting Simulation (Figure 4) activity, which permits learners to test and evaluate the effects of street lighting through colour rendition on a typical street scene. This simulation provides learners with a realistic security scenario to which they can apply their knowledge about illumination.

Graduate Attributes

In addition to the subject content and professional knowledge, the field of security, embraces a large number of generic skills such as critical thinking, problem solving, and the interpretation of information that prepare learners for a variety of careers in government agencies, social services and industry (Hosie, Smith & Luca 2003). Professional endorsement and accreditation has been received for the knowledge domains that are addressed by each component of the Graduate Certificate in Security Management. This has resulted in benefits such as industry recognition, endorsed standards, and ultimately, quality educational programs. The formal knowledge of security processes provides an ideal basis for specific attributes that a graduate of this course is expected to attain. Mapping the appropriate Graduate Attributes across the course provides a framework for structuring learning events and learning outcomes. This has been achieved by documenting the common practice across the curriculum and then extending the development of attributes to related units of the course.

Graduate Attributes have been developed to provide desired learning approaches to be embedded into the curriculum for accepted learning outcomes. Ten Graduate Attributes have been adopted by ECU. Four Core Attributes reflect the themes of Service, Professionalism, and Enterprise. The other six Generic Attributes represent the potential for graduates to become a specialist with workplace experience. Mapping the appropriate Graduate Attributes across the course provides a framework for structuring learning events and learning outcomes as being Embedded, Inferred or Implied in the learning process. It is not the intention that all ten attributes be embedded in every unit of study in a course, but rather it is expected that by the time a learner graduates they will have acquired all ten of the attributes by virtue of having completed the course. Table 1 shows the focus areas of each unit.

Table 1
Graduate Attributes: Focus of units in the Graduate Certificate in Security Management

	Graduate Attributes						
	Core Attributes						
Units	**Enterprise, Initiative & Creativity**	**Professional Knowledge**	**Service**	**Workplace Experience or Applied Competencies**	**Awareness of Political, Social & Ethical Issues**	**Communication**	**Interna Cros Av**
SCY 1103/4103 Physical Security		Em	Im	Em		Em	
SCY 2104/4104 Electronic Security 1		Em	Im	Em		Em	
SCY 1101/4101 Security and Risk Management	In	Em	Im	Em	In	Em	In
SCY 1202/4202 Facility Management 1		Em	Im			Em	

Note. Em = Embedded, In = Inferred, and Im = Implied.

The core attributes are thoroughly treated in the units of the Graduate Certificate in Security Management course, while the generic attributes also comprise an important component of the course. The course development facilitated by the Instructional Design process ensures compliance with the Australian Universities Quality Assurance framework (MCEETYA 2002) that supports the creation of effective and innovative learning environments and quality learning resources. These attributes are considered essential to the comprehensive education of all security professionals in SE Asia. Close examination of Table 1 will reveal that these attributes map onto the Crisis Management Model as shown in Figure 1. For example, 'Professional Knowledge', 'Communication' and 'Problem Solving/Decision Making' are all embedded into every unit in the Graduate Certificate in Security Management. These attributes are important components of any 'preparation' program for crisis management to ensure that 'deep learning' occurs, especially when combined with the constant iterative design of learning opportunities about crisis management of the course.

Security Management Course Features

Features in the Graduate Certificate in Security Management course include field scenarios, images, graphics, and video clips, together with security site images of actual security barriers, systems and technologies to simulate learning experiences. These are government security practices that are not usually available for learners to observe because of confidentially requirements. However, for this course national and international government agencies have provided unique learning materials for learners to observe aspects of security. The uniqueness of the online course is a consequence of unit content and its application in the protection of assets. Graphics, simulations, and video clips have been incorporated into the online learning, shown in Figures 2-5, to present aspects of security that are not normally available to learners:

- Defence in Depth principle;
- Flowchart application to Defence in Depth;
- Security lighting simulation; and
- Images and video clips.

The purpose of physical security is to delay an intruder for sufficient time until a response group arrives to apprehend the intruder. This is best achieved by a series of barriers, rather than a strong single barrier. The principle of 'Defence in Depth' imposes a succession of barriers, which require access between the public and the resource. This principle has been developed to gain time for the protection of a facility. Hence, the principle of Defence in Depth may be applied to a facility or building. In practice a succession of barriers are used to protect the valuable assets of the organisation established in a commercial or industrial facility to prevent access by intruders. The purpose of a succession of barriers is to extend the duration taken for the physical security of an installation to be breached. This is achieved according to the following physical security functions: deterrence, delay, detection, and response, where the degree of physical security is in keeping with the value of assets and risks to assets in the establishment.

The delay time of a succession of barriers to be penetrated before the target is attacked, determines the response

time for the apprehension of intruder(s). The strategy relies on the response force being able to arrive at the source of the alarm whilst the intruder(s) are delayed through either the number of delay barriers or the physical strength of the delay barriers. These features of the Defence in Depth strategy are illustrated through the interactive nature of the simulation learning tasks shown in Figures 2-5. Field scenarios have been developed for the activities to make the learning experiences as realistic as possible. The simulations and graphics provide these experiences, together with security site images for actual security barriers, systems and technologies. Instruction has been sequenced within modules and within units of the course. Interactive multimedia is being used to simulate real world models, and to build scenarios with common experiences as a basis for feedback on learning activities.

Online Delivery

The online version of the Graduate Certificate in Security Management course allows for ease of distribution in the international context. Information technology is a potential source of competitive advantage particularly in the international learning community (Hosie & Mazzarol 1997). The initial configuration of unit web sites provides for the essential online elements. The Blackboard™ is the Learning Management System platform adopted which features flexibility and ease of use.

Blackboard

Blackboard is a suite of software products and services that is used to enable and manage a virtual learning environment. Enrolled learners and currently employed staff can login and use a customisable home page that offers a number of personal management tools. Contents and information posted in these areas is applicable to the specific learner cohort. The Discussion Board facility in Blackboard is used for enquiries about administration of the unit and learning resources. The Blackboard software platform encompasses course management, an academic portal and online campus communities.

Digital Drop Box

A feature of the online units is the ability to submit assignments for assessment through the Digital Drop Box facility in Blackboard. This facility permits learners to submit files to a tutor and for the tutor to retrieve and return files to learners. The facility also permits the tutor to upload files for a particular learner or the entire class. For learners the Drop Box is bi-directional, permitting learners to transfer files to the tutor and the tutor to send files to that learner. The tutor's Drop Box is multidirectional, as files can be received from learners enrolled in the online course and in turn sent onto any individual learner, or alternatively to deliver a file to all learners.

Assessment

Assessments of the learning tasks have been designed to ensure that all objectives and competencies are assessed. Assignment tasks integrate the acquisition and application of professional knowledge with other competencies covered by Graduate Attributes (e.g., interpersonal, communications, IT). Learning is situated in contexts that have personal relevance to learners wherever possible (e.g., research, reporting, and problem solving). Assignments have been structured for incremental submission and formative feedback from peers and tutors before final submission for marking.

Progressive Revelation

A 'Progressive Revelation' function is being developed for the Blackboard platform to present review questions, and then to provide model responses after learners have completed answers to the questions. A series of review questions are provided for learners to practice best responses in the learning process. The feedback for review questions is positive and immediate, provides model responses for novice learners, can be undertaken at the learner's discretion, and once developed, but does not increase the necessity for tutors to provide direct feedback to learners. This is an efficient way to provide high quality on demand feedback to learners.

A Blackboard template has been used for all units of study in the project. Other learning resources for the project units have been distributed to participants on CD, together with online links to other relevant sites. The coursework readers accompanying each of the units are distributed in print form, CD, or as online links to the library where electronic forms of the documents are stored. The online web site contains the functional areas that provide the essential elements for online learning and instruction. Blackboard provides flexibility that allows instructors to add other elements of web based learning as required.

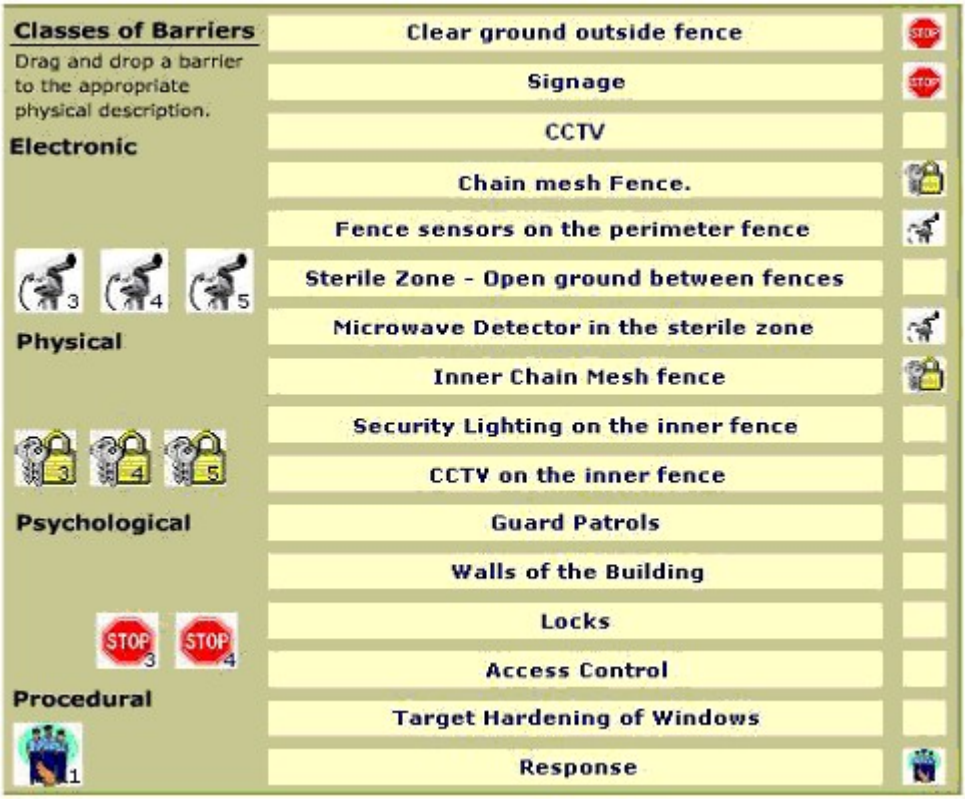
LEARNING SIMULATIONS

Defence in Depth Simulation

The principle of Defence in Depth is applied to a facility or building with a succession of barriers to protect the valuable assets of the organisation. The strategy of a succession of barriers, rather than a single strong barrier, can be applied to a commercial or industrial situation in order to prevent access by intruder(s) (Smith 2002b, Lester & Smith 2003). Field scenarios have been developed for the activities to make the learning experiences as realistic as possible. The simulations and graphics provide these experiences, together with security site images of actual security barriers, systems and technologies.

The principle of Defence in Depth is applied in Figure 2, where learners are instructed to (1) drag and (2) drop an icon barrier onto the chart describing the Defence in Depth strategy for a particular type of facility. Icons must be placed in the correct type sequence before the exercise can be completed. This activity requires the participant to design and develop a Defence in Depth strategy according to the prevention phase of the Crisis Management Model strategy. HRM managers can apply the interactive learning activity in a direct problem solving task to prevent a crisis arising in the organisation or facility.

Figure 2
Defence in Depth Principle: Dragging and Dropping Icons to Construct the Strategy



Defence in Depth Principle

The purpose of physical security is to delay an intruder by barriers for sufficient time until a response group arrives to apprehend the intruder. In Figure 3, the activity requires the learners to progress in the correct sequence, starting at the outside barrier and progressively working into the centre of the 'square onion', for a response with additional information to be displayed for each barrier in the panel at the bottom of the diagram. The Figure 3 shows that the Principle of Defence in Depth imposes a succession of barriers, which require access, between an intruder and the resource.

Figure 3
Defence in Depth Principle

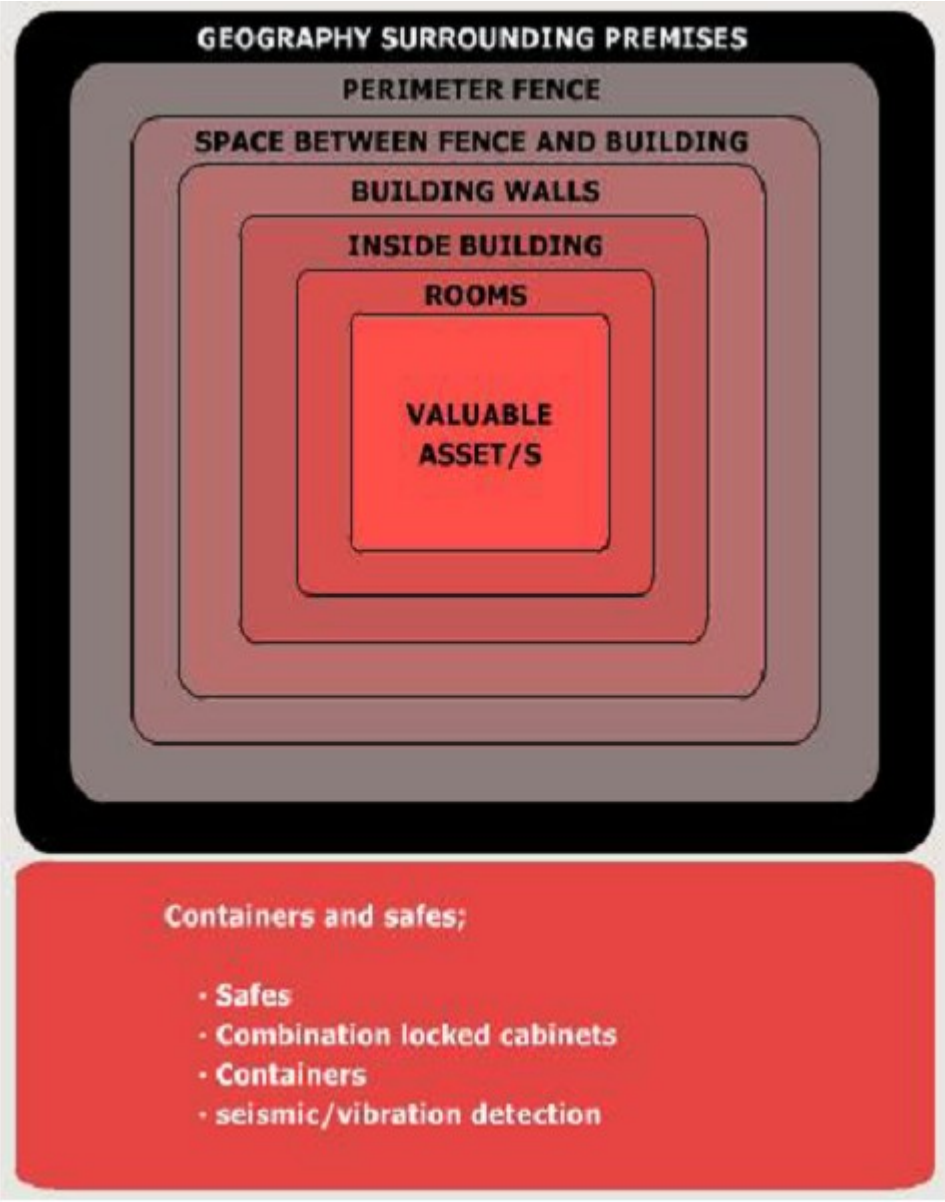


Figure 3 shows the conceptual presentation of the Defence in Depth principle, as applied to typical valuable assets of an organisation, has been developed to gain time for the protection of a facility (Alach & Smith 2002) for:

- Deterrence
- Detection
- Delay
- Response

Again, the prevention phase of the Crisis Management Model is developed by participants learning the strategies for preventing intruder access. This requires organisations to integrate a range of approaches as illustrated in Figures 2 and 3.

Security Lighting Simulation

The Security Lighting Simulation activity provides an opportunity for learners to test and evaluate the effects of street lighting through intensity of illumination and colour rendition on a typical street scene. The purpose of the simulation activity is to reinforce the concepts of surveillance with the intention of observing fine detail from the observation, within the limitations of the physical environment (Figure 4). The simulated street scene appears as a view from the monitor of a CCTV camera with a reasonable field of view and depth of field in focus. The learner has the ability to change the lighting levels on the scene and to observe the degradation of information that is observed as the type and intensity of illumination decreases. Learners are required to record objects in the image that cannot be observed with clarity when the levels of illumination are decreased or different types of light sources are used. Learners are challenged to judge the effectiveness of the camera image in reduced illumination of the scene.

The quality of the illumination can also be changed to simulate the various types of lamps used in street lighting. The illumination quality is determined by distribution of radiation frequencies in the spectrum of the illumination light. The activity simulates the illumination from incandescent, fluorescent, mercury, sodium and metal halide light sources. The effect of colour rendition is observed on the coloured objects in the surveillance image due to the

distribution of frequencies in the illuminating radiation. Learners are required to record the apparent colours of the objects suffering colour rendition. It is important for learners to understand this effect in surveillance as incorrect colour identification has an impact on court evidence. As such, the security lighting simulation challenges learners to apply the information about the quality of illumination to a realistic security scenario.

Colour rendition can affect the identification of potential terrorist threats. For example, the 'colour' of a vehicle varies depending on the source of illumination source (incandescent, fluorescent, mercury, sodium and metal halide) and has the potential to effect the early detection and identification off a possible terrorist car or truck bomb threat. Learners are also 'illuminated' as they explore the various effects of each type and intensity of lights possible with this simulation. Also, the rate of application of CCTV surveillance of scenes continues to increase as a means of monitoring areas of open space for the detection of intruders. CCTV represents a barrier in the Defence in Depth strategy and, as such, will enhance the Crisis Management Model in the prevention phase.

Security System Testing Video Clips

Physical security systems are often tested to destruction in order to determine the capability of the system to delay a determined intruder. These tests are conducted by government agencies, and the outcomes have become part of the national security database. A selection of video clips of physical security systems being tested have been embedded into the online learning materials, in order to provide learners with scenes and images that would not normally be available to public learners. Hence, they require password access to ensure control has been applied to the learning materials. A databank of learning objects has been created from available still and moving images to illustrate facets and activities in security that are either too dangerous, expensive or are inaccessible to learners. These learning objects have been acquired with permission from government agencies and security manufacturers in North America, Europe and Australia and are normally not available to learners.

Figure 4
Security Lighting Simulation of a CCTV Image of a Street Scene

A selection of unique and relevant scenes and images has also been presented for learners to enhance the understanding of the major concepts of the topics. These scenes and images present pictures of actual facilities that participants normally would not have the opportunity to see. For example, Figure 5 shows a scene from a video clip of procedural and physical security barriers at an airport to emphasise the nature of the physical security applied to the Defence in Depth strategy. Again, these images and scenes provide scenarios for learners on methodologies for acquiring security in the Crisis Management Model context.

Figure 5
Video Clip Showing Airport Security

Opportunities for Learner Collaboration

The Discussion Board in Blackboard is used for enquiries about administration of the unit and about learning resources. Contents and information posted in these areas is applicable to the specific learner cohort. One learner's comment was indicative of the feedback on using the communications capabilities of Blackboard: "I would like to see more interactions with learners. I think this would benefit the group. I have found the course sometimes limited by non-discussion with other students." The Blackboard environment is ideally suited to learner collaboration to create products that cannot be produced individually. Discussions of views or ideas would greatly enhance the experience. A number of learners also commented on the potential value of synchronous and asynchronous interaction with tutors and other learners. Blackboard provides a chat room for participants which could be utilised for these types of discussions.

Invariably, security learners are already practitioners in the field and this makes for an ideal opportunity for the collaboratively constructing knowledge. A structured approach to collaboration initiated by the tutor would seem to be in order. Moreover, an opportunity is apparent for incorporating a 'learning community' into the design framework (Brook & Oliver 2003). Developing online learning for the security management community could be used to encourage the collaborative construction of knowledge and to contribute to the practices of experienced professionals working in the field. As Moore and Brooks (2000:140) observe, a learning community is "characterised by a willingness of members to share resources, accept and encourage new membership, regular communication, systematic problem solving and preparedness to share success". In this situation, knowledge may be generated though structured and unstructured learning interactions using Blackboard's communications facilities.

DISCUSSION

There are several areas in SE Asia where physical security is threatened. Indeed, SE Asia has already seen a number of planned and successful terrorist attacks, such as the planned, but foiled, bombing plot on the American, Australian, British and Israeli embassies in Singapore (Kelly 2000), the car bombing of the Marriott Hotel in Jakarta (Elegant 2003), the Bali bombing (Shubert 2003), the bombing of the Australian embassy in Jakarta (Palmer 2004), along with various other insurgent activities in the region. In all of these instances, both physical and human targets were exposed. Experience has now shown that all strategic installations are potential terrorist targets.

Embassies, consulates and other strategic installations, such as large container ports and petrochemical plants, are ready soft targets for terrorist and criminal attack. Moreover, container vessels manned by small crews operating in isolated locations in the Malacca Straits and South China Sea are amongst the latest threats (Ramachandran 2004). A key terrorism target is the 900 kilometre Malacca Straits located between Indonesia, Malaysia and Singapore. A quarter of the world's ship borne trade and half of its oil pass through the Strait. An attack on large vessels has the potential to disrupt world trade at an enormous economic cost and severally impact on people's lives.

Arguably, education about crisis management needs to be based on an established model of practice, such as the PPRR (Heck 1991, Rosental & Pijnenberg 1991) as shown in Figure 1. To be effective it is asserted that learning should be integrated with the prevention, preparation, response and recovery aspects of organisations' responses to crisis management. As such, this learning needs to permeate the entire HRM function. Double loop learning needs to be embedded into every cycle of an organisation's crisis management process to ensure that organisational deep learning and subsequent change in management policies and practices occurs. This entails making a concerted management changes in a period of indifferent economic circumstances for some countries in the region. Part of this mindshift lies in accepting that 'blended learning' (Rossett, Douglis & Frazee 2003) has the potential to an effective and efficient way of delivering consistent and high quality learning to a large number of learners in distributed locations.

Technologically Mediated Learning is an efficacious way of delivering training that can be designed to be more flexible and supportive of the principles of adult learning (Bennett & Reilly 1993). Since 9/11 companies have become interested in the potential of new technologies to offer more effective and efficient ways of providing education to staff (Caudron 2002). Important transactional considerations, such as the reduction training time and the lowering of travel costs (and risks) and time away from the workplace, have also become an important driver for adopting technological solutions for training. A trend to online learning is a strong expression of Technologically Mediated Learning, such as videoconferencing, webconferencing, learning content management systems and the use of digital storage technologies (e.g., CD-ROMs, DVDs).

Technologically Mediated Learning satisfies the criteria for delivering high quality learning that is 'defensible' in terms of ensuring an effective universal standard of quality learning experiences are being delivered. Proponents of online learning extol the virtues of its capacity for accessibility, timeliness, consistent quality, convenience and interactivity, but invariably miss a critical point. Quality online experiences will only be achieved if robust Instructional Design principles are embedded in the development of these learning materials (Reigeluth 1999, Smith & Ragan 1999). Commitment to designing, developing and evaluating quality online materials is essential to realise the desired learning gains.

Terrorism has affected the way that organisations conceive and treat learning. In the post-terrorist era many organisations have opted to implement Technologically Mediated Learning, particularly online learning. As Caudron (2002) so elegantly puts the situation post 9/11:

> Overnight, or so it seemed, the pumpkin of technology was transformed into a gleaming chariot ready to deliver to companies to new cost effective heights of learning technology. Of course technology based training has been idling at the curb for along time, and usage in all forms has been steadily accelerating. (p.27)

This rapidly emerging trend to utilise cost-effective and appropriate technology is being driven by need for employees to go beyond provision of reactive and periodic learning experiences to the necessity of being constantly well informed and prepared. Responses to bioterrorism threats must be rapid and effective to avoid tragedy. Caudron (2002: 30) accurately observed that "technology in all its various forms has taken up a permanent and vastly more influential residence within the training function." As priorities for meeting terrorist threats change by the minute, rather than the daily, institutions need that are more efficient users of technology are likely to become 'learning organisations' (Senge 1990, Price 2000) with greater survival potential.

Distributed technologies, such as the Internet, are appropriate for learning in organisations in SE Asia. Indeed, as many transnational organisations are based in SE Asia this is an efficacious way of delivering learning to employees distributed across the world. However, it is imperative that learners in SE Asia are not just passive consumers of online courses developed in the Australia, USA and Europe, but are actively involved in developing and reverse exporting expertise in online learning related to crisis management. Along with American systems of management comes the cultural antecedents transmitted by online learning experiences. These are heavily culturally laden and not always appropriate to the managerial context of SE Asia. A number of countries in SE Asia (e.g., Singapore, Malaysia, Hong Kong) have become ready adopters of technology and are well placed to develop generic and specific learning experiences using a variety of technology (e.g., Hodgeson & Lam 2004). The case study of the physical security training is an example of creative expertise that has been developed in Australian higher education.

The philosophy and pedagogy underlying the design and development of these security management online units is described, and examples are provided of the interactive activities from the physical security unit. Features of the online units in the course include graphics, simulations, and videos to present aspects of security that are not normally available to learners. Learning materials developed for this course have unique attributes as they were specifically designed to provide simulations and interactivity in the learning process for the protection of assets. There are early signs to indicate positive learner experiences with the security learning materials delivered online. This course has also been well received by the international security industry.

Australian universities with offshore teaching programs have gained a competitive advantage in international markets using existing and emerging information technologies to package and deliver interactive educational services on demand over long distances (Mazzarol & Hosie 1997). The materials in the Security Management course have unique attributes as they were specifically designed to provide simulations and interactivity in the learning process. Field scenarios have been developed for the activities to make the learning experiences as realistic as possible. The simulations and graphics provide these experiences, together with security site images for actual security barriers, systems and technologies.

Course Review

Overall, there was a favourable response to delivering the Security Management units online. The course participants were located throughout Australia, and in overseas locations such as Hong Kong, Singapore, Africa, Malaysia and Ireland. Initial feedback indicates that the quality of the materials produced is beyond what is usual, with high ratings on learner-centred environments, engaging, richness, inclusivity, and meaningful assessments (Hosie et al. 2004). Learner's feedback is already being used to modify the courseware as part of the quality initiatives. Areas for improvement were also identified, such as structured online discussions and extended use of Blackboard features. Procedures derived from the Online Quality Guidelines (Oliver & Herrington 2001) have been incorporated into product reviews and the first units.

Analysis of regularly collected findings is being used formatively to both revise existing materials and approaches in SE Asian learning contexts, and to inform the design of new units. More data and feedback are needed before trends can be ascertained. Preparedness is an important mindset and practical defence for organisations in SE Asia which are likely to be concerned about potential terrorist events. Constructivist learning is relatively new way of approaching online eLearning in SE Asia. Future evaluations of the security course will assess the appropriateness of a constructivist approach to learning about security management in the SE Asian context.

CONCLUSION

Effective crisis management is vital for the survival and prosperity of organisations. Preparedness is important for organisations concerned about preventing terrorist events. As experience has now shown all strategic installations are potential terrorist targets. Education about security management is an important part of crisis management in preparation for terrorist events. High quality security management education is a priority for government and industry both within SE Asia and in the international context. Security management education seeks to provide the content and generic skills and the knowledge necessary for the protection of the assets of organisations and individuals through appropriate learning approaches. The field of security, in addition to the subject/professional knowledge, embraces a large number of generic skills to prepare learners and employees for a variety of careers in government agencies, social services and industry. The featured physical security unit presents the principles underlying the protection of assets of an organisation, and will encourage the learner to seek examples and applications of the security practices in the community. The emphasis is on best practice through reducing the risk of asset loss from high threat situations.

Organisations are now finally realising that Technologically Mediated Learning saves learning costs and can be delivered far more flexibly than tradition methods of orchestrating learning. There is likely to be an increasingly rapid uptake of the use of online learning for organisations preparing for crisis management in SE Asia. Technologically Mediated Learning is an effective way of delivering such education online. Before embarking on developing online education, it is essential to undertake a needs analysis which should underpin quality Instructional Design of the learning materials to ensure that effective learning occurs. Issues relating to online learning design development considerations need to be fully explored, including: the philosophy and pedagogy informing the design; the main learning outcomes expected; attributes expected of learners; a well conceived framework for designing and evaluating such courses that reflect the high quality Instructional Design. Online learning using graphics simulations is an ideal way of ensuring that deep learning is achieved to a consistent standard.

There is potential to integrate rapidly emerging Technologically Mediated Learning into SE Asian courses in crisis management. A case is made for using distributed technologies for learning, but with the caveat that technological determinism does not become an opportunity for cultural imperialism. Alternatively, organisations in SE Asia may opt to develop their education in preparation for crisis management. Education about security management is an important part of preparing for terrorist events and future research will determine how well this approach will integrate into a SE Asian learning context.

AUTHORS

Dr Peter Hosie is a Post Doctoral Research Fellow at Curtin Business School, Curtin University of Technology. Peter has published over 50 articles and reports on Technologically-Mediated Learning and HRM/HRD. His work has been cited in over 40 international articles, papers and reports.

E-Mail: Peter.Hosie@cbs.curtin.edu.au

Dr Clifton Smith is an Associate Professor, Security Science in the School of Engineering and Mathematics, Edith Cowan University. Professor Smith conducts research in ballistics imaging, IT security, biometric imaging, and security education. He has published extensively in these research areas, and has developed professional security education programs.

E-Mail: clifton.smith@ecu.edu.au

REFERENCES

Alach, Z., & Smith, C.L. (2002). A suggestion for a holistic (descriptive) approach to modelling physical security decisions. *Proceedings of 3rd Australian Information Warfare and Security Conference*, 107-116.

Argyris, C. (1993). *Knowledge for action: A guide to overcoming barriers to organizational change*. San Francisco: Jossey Bass.

Argyris, C., & Schön, D. (1974). *Theory in practice. Increasing professional effectiveness*, San Francisco: Jossey-Bass.

Bennett, S., & Reilly, P. (1993). Using interactive multimedia to improve operator training at Queensland Alumina Limited. *Australian Journal of Educational Technology*, 14(2), 75-87. http://www.ascilite.org.au/ajet/ajet14/bennett.html

Brook, C., & Oliver, R. (2003). Online learning communities: Investigating a design framework. *Australian Journal of Educational Technology*, 19(2), 139-160.

Brown, M.D. (2004). *NIMS: The Lasting Legacy of 9/11*. Under Secretary of Homeland Security for Emergency US Government. 6/3/04. (http://www.firefighting.com/articles/namFullView.asp?namID=9864)

Caudron, S. (2002). Training in a post-terrorist era. *Training and Development*, Feb, 25-30.

Creelman, D. (2004). Interview: Ian Mitroff on Crisis Leadership, *HR.Com* (http://www.hr.com/HRcom/index.cfm/WeeklyMag/9A954EE7-B500-4AC4-A13DF077B83214E2?ost=wmFeature)

Dalgarno, B.J. (1996). Constructivist Computer Assisted Learning: Theory and Techniques. In A. Christie, P. James, & B. Vaughan (Eds.), *Making New Connections*. Proceedings of ASCILITE '96. Adelaide, University of South Australia.

Elegant, S. (2003). New Wave Of Terror? A deadly Jakarta bombing raises questions about the effectiveness of Indonesia's antiterror measures. *Timeasia*. August 18-25, 2003 / 162 (6). (http://www.time.com/time/asia/magazine/printout/0,13675,501030818-474520,00.html)

Heath, R. (1993). Dealing with complete crisis-the crisis management shell structure. *Safety Science*, 30, 139-150.

Heck, J.P. (1991). Comments on "The Zeebrugge ferry distaer". In Rosenthal, U., & Pijnenberg, B. (Eds.), *Crisis Management and Decision Making*. Kluwer, Dordrecht.

Hesse, L., & Smith, C.L. (2001). *Core curriculum in Security Science.* Proceedings of the 2nd World Conference on Information Security Education, 129-146.

Hodgeson, P., & Lam, P. (2004). Quality management of a joint-university e-learning project. *Global Educator*, July, 1-6. (http://www.globaled.com/articles.html).

Hosie, P. (1993). Technologically mediated learning: The future of training in Australia. *Australian Journal of Educational Technology*, 9(1), 69-86.

Hosie, P. (1994). Human resource managers and training-A peek into the future. In A. Nankervis & R. Compton (Eds.), *Readings in Strategic Human Resource Management* (259-277). Sydney: Thomas Nelson.

Hosie, P., & Mazzarol, T. (1997). Using technology for the competitive delivery of education services. *Journal of Computer Assisted Learning*, 15(2), 174-180.

Hosie, P., Mazzarol, T. & Jacobs, S. (1998). Information technology as a source of competitive advantage in international education. *Journal of Information Technology and Teacher Education*, 17(1), 113-128.

Hosie, P., & Smith, C. & Luca, J. (2003). Security management education online. ASCILITE 2003. *INTERACT-INTEGRATE-IMPACT*, 7-10 December, Adelaide, Adelaide University.

Kelley, J. (2000). *Malaysia site of Sept. 11 plotting*, FBI report says, USA TODAY. 01/29/2002. (http://pgoh.free.fr/fbi_nyt.html)

Lester, A.J., & Smith, C.L. (2003). An investigation into the application of Defence in Depth theory to electronic information protection. *Journal of Information Warfare*, 2(2), 88-96.

Mazzarol, T., & Hosie, P. (1997). Long distance teaching: The impact of offshore programs and information technology on academic work. *Australian Universities Review*, 40(1), 20-24.

MCEETYA. (2002). *Australian qualifications framework*. Australian Qualifications Framework (AQF) Advisory Board, Carlton South Australian Qualifications Framework Advisory Board to MCEETYA, (http: / /www.aqf.edu.au)

Mitroff, I. I. (2004). *Crisis leadership: Planning for the unthinkable.* University of Southern California.

Moore, A.B. & Brooks, R. (2000). Learning communities and community development: Describing the process. *Learning Communities: International Journal of Adult and Vocational Learning*, 1(1), 15.

Moshman, D. (1982). Exogenous, Endogenous and Dialectical Constructivism. *Developmental Review*, 2, 371-384.

Oliver, R. & Herrington, J. (2001). teaching and learning online: a beginner's guide to e-learning and e-teaching in higher education. *Centre for Research in Information Technology and Communications*, Edith Cowan University, Western Australia.

Palmer, T. (2004). *At least eight killed in embassy attack*, ABC NEWS ONLINE. (http://www.abc.net.au/news/newsitems/s1195760.htm)

Pricewaterhouse Coopers (2001). Lessons Learned From September 11, 2001. *Presentation To The Audit Committee Of The Johns Hopkins Health* (http://It.Jhu.Edu/Divisions/Etso/Engineeringservices/Securitydisaster/Disaster/911lessons.Html)

Price, A. (2000). *Principles of human resource management: An action-learning approach*. Oxford: Blackwell.

Ramachandran, S. (2004). Divisions over terror threat in Malacca Straits, *Online Asia Times*. 16 June 2004 (http://www.atimes.com/atimes/Southeast_Asia/FF16Ae01.html)

Reigeluth, C.M. (1999). What is instructional-design theory, and how is it changing?. In C.M. Reigeluth (Ed.), *Instructional-design theories and models: A new paradigm of instructional theory* (Vol.ii,425-459). Hillsdale, NJ: Lawrence Erlbaum Associates.

Rosental, U., & Pijnenberg, B. (1991). *Crisis management and decision making*. Kluwer: Dordrecht.

Rossett, A, Douglis, F, & Frazee, R. (2003). Strategies for building blended learning, *Learning Circuits*. (http://www.learningcircuits.org/2003/jul2003/rossett.htm)

Senge, P.M. (1990). *The fifth discipline: The art and practice of the learning organization*. New York: Doubleday.

Shubert, A. (2003). Bali bombing suspect admits role, *CNN Correspondent*. Thursday, May 29, 2003. (http://www.cnn.com/2003/WORLD/asiapcf/southeast/05/29/bali.trial/_

Smith, C.L. (2001). Security Science as an applied science? *Australian Science Teachers Journal*, 47(2), 32-36.

Smith, C.L. (2002a). Security Science - An emerging applied science. *SCIOS*, 37(2), 8-10.

Smith, C.L. (2002b). A method for understanding students' perceptions of concepts in the Defence in Depth strategy. *Proceedings of 3rd Australian Information Warfare and Security Conference*, 19-27.

Smith, P.L., & Ragan, T. (1999). *Instructional design*. New York: John Wiley & Sons.

Smith, C.L., & Robinson, M. (1999). The understanding of security technology and its applications. *Proceedings of the IEEE International Carnahan Conference on Security Technology*, Madrid, Spain.

Steffe, L.P., & Gale, J. (Eds.), (1995). *Constructivism in education*. Hillsdale, NJ: Lawrence Erlaum Associates.

APPENDIX 1

Suspected al-Qaeda Terrorist Acts

1993 (Feb):	Bombing of World Trade Center (WTC); 6 killed.
1993 (Oct):	Killing of U.S. soldiers in Somalia.
1996 (June):	Truck bombing at Khobar Towers barracks in Dhahran, Saudi Arabia, kills 19 Americans.
1998 (Aug):	Bombing of U.S. embassies in East Africa; 224 killed, including 12 Americans.
1999 (Dec):	Plot to bomb millennium celebrations in Seattle foiled when customs agents arrest an Algerian smuggling explosives into the U.S.
2000 (Oct):	Bombing of the USS Cole in port in Yemen; 17 U.S. sailors killed.
2001 (Sept):	Destruction of WTC, Pentagon attack. Total dead 3,044.
2002 (Apr):	Explosion at historic synagogue in Tunisia leaves 21 dead, including 14 German tourists.
2002 (May):	Car explodes outside hotel in Karachi, Pakistan, killing 14, including 11 French citizens.
2002 (June):	Bomb explodes outside American Consulate in Karachi, Pakistan, killing 12.
2002 (Oct):	Nightclub bombings in Bali, Indonesia, kill 202, mostly Australian citizens.

2002 (Nov):	Suicide attack on a hotel in Mombasa, Kenya, kills 16.
2003 (May):	Suicide bombers kill 34, including 8 Americans, at housing compounds for Westerners in Riyadh, Saudi Arabia.
2003 (May):	Four bombs kill 24 people, targeting Jewish, Spanish, and Belgian sites in Casablanca, Morocco.
2003 (Aug):	Suicide car bomb kills 12, injures 150, at Marriott Hotel in Jakarta, Indonesia.
2003 (Nov):	Explosions rock a Riyadh, Saudi Arabia housing compound killing 17.
2003 (Nov):	Suicide car bombers simultaneously attack two synagogues in Istanbul, Turkey, killing 25 and injuring hundreds.
2004 (Mar):	Ten terrorists' bombs exploded almost simultaneously during the morning rush hour in Madrid, Spain, killing 190 and injuring more than 1,800.
2004 (Sept):	A car bomb has exploded outside the Australian embassy in Jakarta killing at least eight people and wounding more than 160 in an attack police have blamed on al Qaeda-linked militants.

APPENDIX 2

Lessons Learned From September 11, 2001

ASSESS ADEQUACY: Reassess the robustness of plan and recovery strategies

INTEGRATE AND MAINTAIN PLANS: Ensure that the Crisis Management, Business Continuity and Disaster Recovery Plans are integrated within the institution and tested in a realistic and integrated manner. Organizations are in a constant state of change. Develop a disciplined approach to reflect changed circumstances in plans.

INCREASE KNOWLEDGE: Educate staff in their role in recovery and the institutions approach to recovery. Increase awareness, training and testing.

CONSIDER THE ENTIRE SUPPLY CHAIN: Integrate key customers and suppliers into your plans. They need to know where you will be and you need to know where they will be.

PLAN FOR REALISTIC SCENARIOS: Focus on the worst case, worst time of the year and do not assume away issues (e.g. "All key suppliers and our bank have plans. We don't need to worry about them being available.")

CREATE A CULTURE OF CONTINUITY: Develop a culture that treats continuity as part of every project and decision, not as a separate issue.

(Pricewaterhouse Coopers 2001)