2003

Security management education online

Peter J. Hosie
Edith Cowan University

Clifton L. Smith
Edith Cowan University

Joseph Luca
Edith Cowan University

INTERACT
INTEGRATE
IMPACT

Proceedings of the 20th Annual Conference of the Australasian Society for Computers in Learning in Tertiary Education (ASCILITE)

Adelaide, Australia
7–10 December 2003

Editors
Geoffrey Crisp, Di Thiele, Ingrid Scholten, Sandra Barker, Judi Baron

Citations of works should have the following format:

Author, A. & Writer B. (2003). Paper title: What it's called. In G.Crisp, D.Thiele, I.Scholten, S.Barker and J.Baron (Eds), *Interact, Integrate, Impact: Proceedings of the 20th Annual Conference of the Australasian Society for Computers in Learning in Tertiary Education*. Adelaide, 7-10 December 2003.

ISBN CDROM 0-9751702-1-X WEB 0-9751702-2-8

ascilite
Australasian Society For Computers
In Learning In Tertiary Education

Published by ASCILITE www.ascilite.org.au

SECURITY MANAGEMENT EDUCATION ONLINE

Peter J Hosie
Learning Development Services
Edith Cowan University, AUSTRALIA
p.hosie@ecu.edu.au

Clifton L Smith
School of Engineering and Mathematics
Edith Cowan University, AUSTRALIA
cliflton.smith@ecu.edu.au

Joe Luca
School of Communications and Multimedia
Edith Cowan University, AUSTRALIA
j.luca@cowan.edu.au

Abstract

This paper describes the philosophy and pedagogy informing the design and development of Security Science online units. The Physical Security unit is used to illustrate the development of the online learning strategies and interactive activities. Learning materials developed for this 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. Simulations and graphics provide these experiences, together with security site images for actual security barriers, systems and technologies. Features of units in the course include graphics, simulations, and video clips to present learning aspects of security that are not normally available to students.

Keywords

Security Science, Physical Security, online, interactive, simulation, graphics, video clips.

Education about terrorism

Terrorist tragedies in Kenya (2001), New York, Washington (s9/11), Bali (2002), Morocco and Saudi Arabia (2003) have emphasised the need for high quality professional education in security risk and security technology for the protection of assets. These events have focussed national and international attention on the necessity for professional security education for government, private organisations, and community services. Although the extent of the security industry in Australia is considerable (five fold on the total of all police services in Australia) it has a relatively small professional component of education.

Since the terrorism events, the international and Australian governments have realised the necessity for professional education of personnel in security technology, security management, and security risk to protect assets in national security facilities. The Security Science programme in the School of Engineering and Mathematics at Edith Cowan University (ECU) has been established on the themes of security technology, security risk, and security management. The undergraduate courses have been offered at ECU for ten years and have developed both a national and international reputation for providing quality learning experience for students. Security Science at ECU is widely recognised in the national and international contexts by both government and industry[1]. As a consequence, the development of online security units has been well received by the international security industry.

[1] Dr Smith has received the Institute of Electrical and Electronic Engineers Kentucky Award for contribution to security education and the Australian Security Industry Association (Ltd) national award for contribution to Security education. ECU students have been placed first or second for the first three years of undergraduate/postgraduate essay competition for the American Society of Industrial Security, the largest international professional security association.

All undergraduate Security Science courses at ECU are currently being delivered by distance learning, using print-based materials. As a consequence, distance education students from all continents are enrolled in these courses, as well as a considerable enrolment in the eastern states of Australia. The terrorist events in USA, Africa and Bali have had the effect of considerably increasing the demand for Security Science courses. Effective education is becoming increasingly important to Australian industry because of the legal responsibility of a company to ensure that employees have adequate education to carry out their work safely and the need to achieve a competitive advantage through increased productivity (Hosie, 1993).

ECU Strategic Online Projects

Strategic Online Project target courses, such as the Security Science, are of particular strategic importance for ECU because of their potential to function as high-quality exemplars and to allow global distribution of learning materials. The Strategic Online Project has selected course development proposals through a competitive process where the proposals were required to demonstrate how they would meet specified objectives:

- The products created will demonstrate high quality DEST Mode B (online with other learning resources) and Mode C (exclusively online) teaching and learning.
- The products created will generate income through enrolment.
- The projects will incorporate relevant professional development and course improvement to meet ECU's Online Quality Guidelines (http://www.ecu.edu.au/lds/rd/units/quality_guidelines.html).

Key Features of Successful Strategic Online Projects

The factors that have been identified that contribute significantly to the success of the project include:

- Project leaders and teams have had prior online teaching experience. They have a good sense of the scope of work that is required, and can anticipate what is needed for effective online units.
- Project staff engage fully in planning the online learning environment they want to create, and developing unit specifications. This work precedes any unit development, and typically is a three month period of time.

The adaptation or development of online units of study was controlled by Project Leaders who accessed Instructional Designers as consultants and facilitators. Project Teams engaged in appropriate professional development before embarking on unit development. (http://www.ecu.edu.au/lds/rd/sop/)

Structure of the Security Science course

The demand for Security Science courses in the national and international contexts is considerable. Security at ECU has been providing professional education for the protection of human and physical assets in the international and national domains. This project is an extension of these courses and has developed the online learning resources for the four security science units of the Graduate/Executive Certificate in Security Management.

The units of study in the Graduate/Executive Certificate in the Security Science course provide an emphasis on best practice through reducing the risk of asset loss from high threat situations, which 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.
- ***Electronic Security 1***: 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.

Major learning outcomes: Graduate Attributes

ECU has adopted ten Graduate Attributes. Four of ECU's Core Attributes reflect the University's themes of *Service, Professionalism, and Enterprise*. The six Generic attributes represent the potential for ECU graduates to become a specialist in providing graduates with workplace experience. Graduate Attributes have been developed to provide desired learning approaches for courses at ECU, and are embedded into the curriculum for accepted learning outcomes. Mapping the appropriate Graduate Attributes across the course provides a framework for structuring learning events and learning outcomes. 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 student graduates they have acquired all ten of the attributes by virtue of having completed an ECU course. Table 1 shows the focus areas of each unit.

The core attributes have been thoroughly treated in the units of the Graduate/Executive Certificate in Security Management course, while the generic attributes also indicate a strong component of the course. Also, the course development facilitated by the ECU Instructional Design process ensures compliance with the Australian Universities Quality Assurance framework that supports the creation of effective and innovative learning environments and quality learning resources.

	Graduate Attributes									
	Core Attributes				Generic Attributes					
Units	Enterprise, Initiative & Creativity	Professional Knowledge	Service	Workplace Experience or Applied Competencies	Awareness of Political, Social & Ethical Issues	Communication	Internationalisation/ Cross Cultural Awareness	Problem Solving/ Decision Making	Teamwork	Use of Technology Information Literacy
SCY 1103/4103 **Physical Security**		✓	✓	✓		✓		✓	✓	✓
SCY 2104/4104 **Electronic Security 1**		✓	✓	✓		✓		✓		✓
SCY 1101/4101 **Security and Risk Management**	✓	✓	✓	✓	✓	✓	✓	✓	✓	
SCY 1202/4202 **Facility Management 1**		✓	✓			✓		✓	✓	✓

Table 1: Graduate Attributes: Focus of units in the Graduate /Executive Certificate in Security Science

Levels of Online Learning

Until recently there were no common definitions for describing the different types of "onlineness". Definitions offered by institutions or individuals offered little basis for comparison or usefulness for articulating strategy and developing subsequent business processes. The Australian Federal Department of Employment Training and Youth Affair's (DETYA) describes three modes of online as Web Supplemented (Mode A), Web Dependent (Mode B), and Fully Online (Mode C). These DETYA online definitions have regularised the understanding of the features and components of online delivery units of study, so that students' expectations of levels of utility of the learning materials have been mainly satisfied. According to the DETYA definitions of types of online delivery, the Graduate/Executive Certificate in Security Management units are Mode B, where students interact with the materials, the staff, and other students. These units also have a reading list that is sent to the students to supplement the learning materials.

Features in the Graduate/Executive Certificate in Security Management course include graphics, simulations, and video clips to present aspects of security that are not normally available in this combination to students. Government security practices are not usually available for students to observe because of confidentially requirements. However, for this course national and international government agencies have provided unique materials for students to observe aspects of security. The characteristic of uniqueness of the online course is a consequence of unit content, and the application in the protection of assets. Graphics, simulations, and interactivities have been applied to the following learning activities:

- Defence in depth principle;
- Flowchart application to defence in depth;
- Security lighting simulation;
- Video clips.

Some features of the Physical Security unit are presented to illustrate the typical development of the online course, with learning strategies and interactive activities presented. 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.

Online delivery

The online version of the Graduate/Executive Certificate in Security Management course will also allow for ease of distribution in the international context. As Hosie and Mazzarol (1999) assert, information technology is a potential source of competitive advantage particularly in the international education industry. Instruction has been sequenced within modules and within units of the course. Interactive multimedia is being used in the Mode B instruction to simulate real world models, and to build scenarios with common experiences as a basis for feedback on learning activities. To ensure that the project meets the Mode B requirement, assignments have been structured for incremental submission and formative feedback from peers and tutors before final submission for marking.

A feature of the online units is the ability to submit assignments for assessment through the Digital Drop Box facility in Blackboard (http://www.ecu.edu.au/lds/rd/units/online/blackboard_ecu.html). The Drop Box facility permits students to submit files to a tutor and for the tutor to retrieve and return files to students. The facility also permits the tutor to upload files for a particular student or the entire class. For students the Drop Box is bi-directional permitting students to transfer files to the tutor and the tutor to send files to that student. However, the tutor's Drop Box is multidirectional, as files can be received from students enrolled in the online course and in turn sent onto any individual student, or alternatively to deliver a file to all students. All students enrolled at ECU are allocated an ECU email address although a significant number of students opt to use their own addresses.

My ECU and Blackboard

My ECU is the institution-wide portal to the online learning environment at ECU, developed and implemented using the Blackboard Learning Content Management system. Blackboard is a suite of software products and services that enable and manage a virtual learning environment. The Blackboard software platform encompasses course management, academic portal and online campus communities. All currently enrolled students and currently employed staff can login to and use *My ECU*. It has a customisable home page and offers a number of personal management tools. The page displays a set of standard modules that contain content relevant to each individual user. ECU students obtain access to *My ECU* and its resources when they are enrolled via the enrolment management system (ECUWES), but only units that are created using Blackboard, and in which the student is enrolled, are listed on the student's *My ECU* (http://www.ecu.edu.au/MyECU/). In a similar way, staff have access to *My ECU* when they are recorded as current ECU staff in the HR system, but only Blackboard units in which they have a role are listed on their personalised *My ECU*.

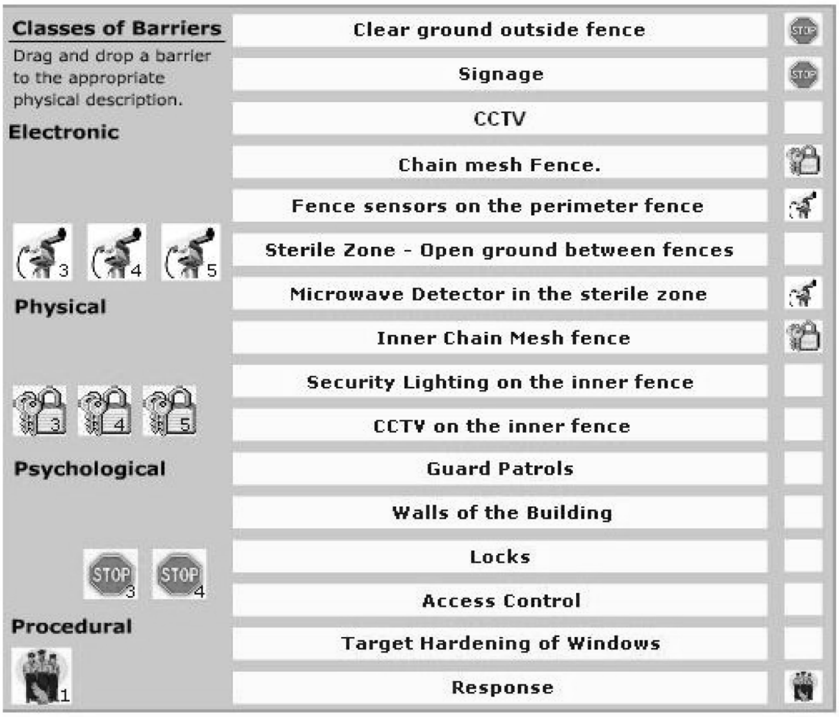
Online Elements

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 ECU and other relevant sites. The coursework Readers accompanying each of the units are distributed in print form, CD, or as online links to the ECU 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 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 intruders. 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. The principle of Defence in Depth is applied in Figure 1, where learners are instructed to drag and drop an icon barrier onto the chart describing the Defence in Depth strategy for a particular type of facility.



Classes of Barriers

Drag and drop a barrier to the appropriate physical description.

Electronic

Physical

Psychological

Procedural

Clear ground outside fence

Signage

CCTV

Chain mesh Fence.

Fence sensors on the perimeter fence

Sterile Zone - Open ground between fences

Microwave Detector in the sterile zone

Inner Chain Mesh fence

Security Lighting on the inner fence

CCTV on the inner fence

Guard Patrols

Walls of the Building

Locks

Access Control

Target Hardening of Windows

Response

Figure 1: Defence in Depth principle where students drag and drop icons to construct the strategy.

Again, the flow chart activity in Figure 2 shows the paths taken for a successful deterrent to an attack on a facility. The diagram is produced by successive clicking on flowchart nodes to indicate input events in the scenario, and possible outcomes from the application of the functions of physical security through the defence in depth functions of:

- Deterrence
- Detection
- Delay
- Response

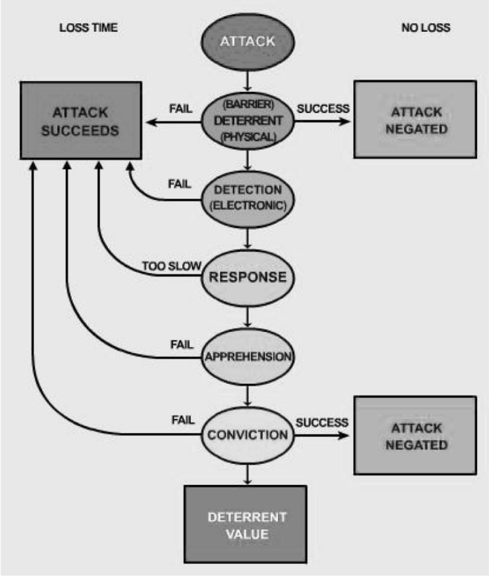


Figure 2: Generic flowchart application to defence in depth to a facility

Security Lighting Simulation

The Security Lighting Simulation activity provides an opportunity for students 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 3). 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 student 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. Students are required to record objects in the image that can not be observed with clarity when the levels of illumination are decreased or different types of light sources are used. Students are encouraged to judge the effectiveness of the camera image in reduced illumination of the scene.

Also, the quality of the illumination can 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. Students are required to record the apparent colours of the objects suffering colour rendition. It is important for students 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. Learners are also illuminated as they explore the various effects of each type and intensity of lights possible with this simulation.

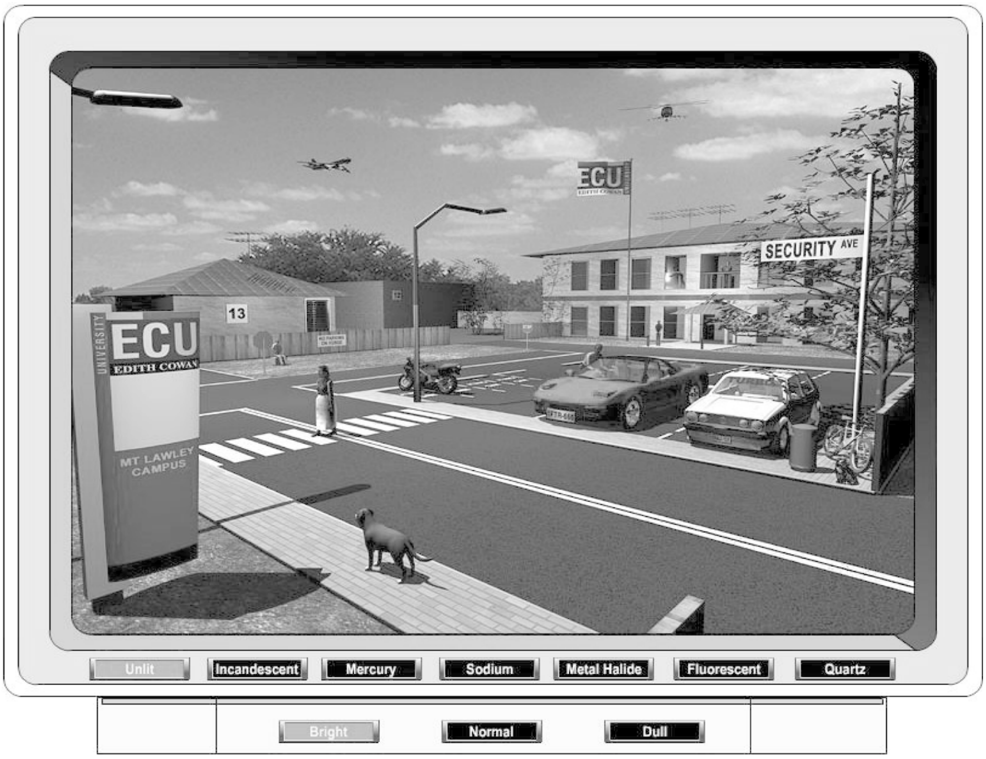


Figure 3: Security lighting simulation of a CCTV image of a street scene.

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. Because these scenes and images are not available to the public, password access 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 students. These learning objects have been acquired with permission from government agencies and manufacturers in North America, Europe and Australia.

Also, a collection of unique and relevant scenes and images has been presented for learners in the units to enhance the understanding of the major concepts of the topics. For example, Figure 4 shows a scene from a video clip of procedural and physical security barriers at an airport.

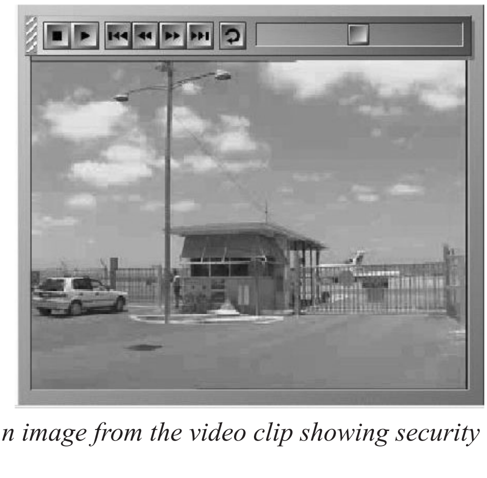


Figure 4: An image from the video clip showing security at an airport

Video clips in this unit worked best on broadband connections (eg. ADSL or dedicated LANs). Delays in loading the videos were experienced by students using a standard Internet Service Providers (eg. 56k modem).

Instructional Design

Figure 5 represents an overview of the process of course design and development documentation that form part of the ECU Instructional Design quality process. This quality process provides the goals, review and communications, planning and quality assurance, and parallel development for online units. This course design and development documentation (Design Documents) ensures that a quality standard of preparation and planning (Unit Specifications) precedes the development of the online units.

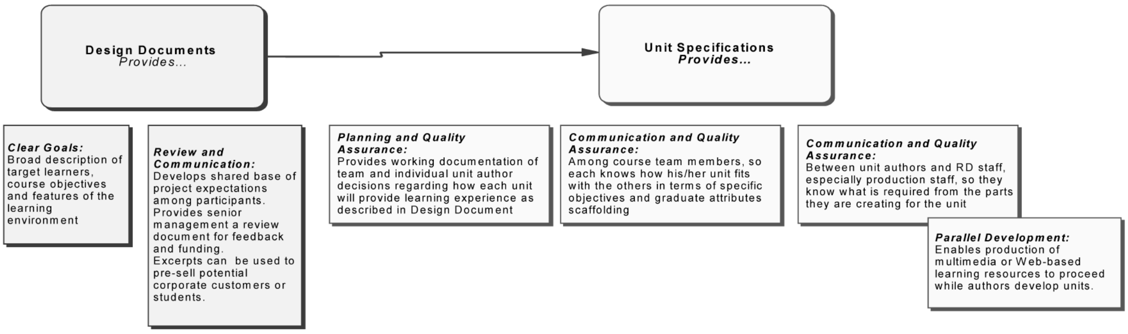

Design Documents
Provides...
Unit Specifications
Provides...
Clear Goals: Broad description of target learners, course objectives and features of the learning environment
Review and Communication: Develops shared base of project expectations among participants. Provides senior management a review document for feedback and funding. Excerpts can be used to pre-sell potential corporate customers or students.
Planning and Quality Assurance: Provides working documentation of team and individual unit author decisions regarding how each unit will provide learning experience as described in Design Document
Communication and Quality Assurance: Among course team members, so each knows how his/her unit fits with the others in terms of specific objectives and graduate attributes scaffolding
Communication and Quality Assurance: Between unit authors and RD staff, especially production staff, so they know what is required from the parts they are creating for the unit
Parallel Development: Enables production of multimedia or Web-based learning resources to proceed while authors develop units.

Figure 5: ECU Instructional Design course design and development documentation
(http://www.ecu.edu.au/lds/pdf/course_design.pdf)

The field of security, in addition to the subject/professional knowledge, embraces a large number of generic skills preparing students for a variety of careers in government agencies, social services and industry. The knowledge domains to be addressed by each component of the course have been endorsed by expert committees to meet the accreditation requirements for core areas of learning.

Flexible learning technologies have been embraced in the development of online Graduate/Executive 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 education 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 a self-directed learning encouraged (Mazzarol & Hosie, 1997). This view also supports the strategy recommended by Rossett and Barnett (1996), who maintain that basic Instructional Design principles must guide the development of computer-based education and recommend an approach based upon analysis, scenarios, discovery and expert advice.

This design primarily adopted an *exogenous constructivism* (Moshman, 1986) approach which recognizes the role of direct instruction but emphasizes 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 2) 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 3) activity, which permits students to test and evaluate the effects of street lighting through colour rendition on a typical street scene. This simulation provides learners with realistic security scenario to which they can apply the information about illumination.

Assessment

Assessments of the learning tasks have been designed to:

- Ensure that all objectives and competencies are assessed.
- Provide a balance of online submissions and invigilated work, as a precaution against cheating.
- Assign tasks that integrate the acquisition and application of professional knowledge with other competencies (eg. interpersonal, communications, IT).
- Situate learning in contexts that have personal relevance to students wherever possible (eg. research, reporting, and problem solving).

ECU Framework for Assessing Quality of Online Learning Materials

Students enrolled in the online course were surveyed with the ECU online quality checklist that was supported by free text questions. A framework has been developed at ECU to provide a means for consistent assessment and evaluation of online learning materials. This framework has been designed in the form of a checklist of items considered to be the critical elements of effective learning environments. The framework is intended to provide users with the capacity to investigate the potential effectiveness of online units through a determination of the scope and extent of these critical elements.

The checklist is based upon the determination of critical elements within three main areas, which describe the complete online setting: *Pedagogies, Resources* and *Delivery*. These learning approaches underpin the unit; the resources contain the content and information that are provided for the learners; and the delivery strategies address issues associated with the ways in which the course is delivered to the learners. The checklist is not intended to be used to deliver a numeric score that provides a definitive evaluation of the courseware. Rather, this checklist is intended to reflect and to indicate areas of the materials that are pedagogically strong and to identify weaknesses that need further attention. Students were also asked about the amount of time devoted to the learning programme, opinions on the interactive activities, and the response rates when accessed remotely.

The ECU quality framework for assessing quality online learning materials is detailed by Oliver, Herrington, (2001) and Herrington, Herrington, Oliver Stoney and Willis (2001). The attributes and assessment framework were developed by the ECU Quality Online Working Group (March, 2001) and describe the essential components of quality online learning materials. ECU is committed to the constructivist approach to learning for both face-to-face and online learning (Steffe & Gale, 1995). Oliver and Herrington (2001) and Herrington, et al. (2001) provide consideration of the critical elements within each of these sections and examples of how these elements can be manifested in online settings.

The students were located throughout Australia, and also overseas in locations, such as Hong Kong and Ireland. Feedback has indicated that the quality of the materials produced is above what is usual, with high ratings on learner-centred environments, engaging, richness, inclusivity, and meaningful assessments. This frequency data provided feedback to adjust the administration and delivery of the units in the course. Given the small sample (N = 9) available it was not possible to extrapolate further from the data on the key areas of: *Pedagogies, Resources* and *Delivery*.

Pedagogies	never	sometimes	always
Authentic tasks The learning activities involve tasks and contexts that reflect the way in which the knowledge will be used in real life settings		4	5
Opportunities for collaboration The environment encourages and requires students to collaborate to create products that could not be produced individually	6	3	
Learner-centred environments There is a focus on activities that provide degrees of freedom, decision-making reflection and self-regulation		4	5
Engaging The learning activities challenge learners and provide some form of encouragement and motivation to support the engagement		5	4
Meaningful assessments Authentic and integrated assessment is used to evaluate students' achievement		5	3
Resources			
Accessibility The resources are organised in ways that make them easily accessed and located	1	7	1
Currency The age of resources are appropriate to the subject matter	1	5	3
Richness The resources reflect a rich variety of perspectives		6	3
Strong use of the media The materials use the various media in appropriate ways	2	6	1
Inclusivity The materials demonstrate cultural and gender inclusivity	2	4	3
Delivery strategies			
Reliable and robust interface The materials are accurate and error free in their operation across all platforms and browsers		7	2
Clear goals, directions and learning plans Unit information and expectation of student roles are clear	1	6	2
Appropriate bandwidth demands The materials download without lengthy delays	3	3	2
Equity and accessibility The unit materials and activities are considerate of students with visual impairment and physical disabilities	1	5	2
Appropriate corporate style The materials use a style that is compatible with ECU policy and guidelines		3	4

(Source: Framework developed by Edith Cowan University Quality Online Working Group, March 2001)

Table 2: Edith Cowan University Quality Online learning quality checklist (N = 9)

As indicated, students are able to submit assignments for formative feedback and assessment using the Digital Drop Box facility in Blackboard. Several technical problems (primarily regarding file sizes of assignments) were experienced with Digital Drop Box, resulting in most students opting to send their assignments as email attachments. A *Progressive Revelation* function is being developed for the Blackboard platform to present review questions, and then provide model responses after students have completed answers to the questions. A series of review questions have been provided for students to practice best responses in the learning process. The feedback for review questions is both positive and immediate, and provides model responses for novice learners.

Opportunities for collaboration

The Discussion Board 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 student cohort. This student's comment was indicative of the feedback on using the communications capabilities of Blackboard: "I would like to see more interactions with students. 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 students to collaborate to create products that could not be produced individually. Discussions of views or ideas would greatly enhance the experience. Blackboard provides a chat room for participants. A number of students also commented on the potential value of synchronous and asynchronous interaction with tutors and other students. 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 (Brooke & 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.

Why are you studying online?

This student's response to the question, "Why did you decide to study this (these) unit(s) online?" provided useful feedback on the nature of identifying and locating a suitable online course to study:

> I have worked for a number of years in the Telecoms fraud environment. My skill set in relation to fraud is high. I have been active on a national level and international level for the last five years in relation to telecoms fraud. I was looking for a new challenge. I have been interested in Physical security and Risk management for a while. I managed to convince my company of the benefits of paying for me to do a course in these topics to raise my skill set and understanding of the various issues. The only issue I found was that in Ireland the courses seemed to be very limited. Through searching online I found the Edith Cowan units. The content within these courses seemed to appeal to me. They thought skills which I could see use for within the environment in which I worked. I also liked the structure of the online access (Blackboard). I have a young son and I already had a full life. I wanted to complete a course structure, which would fit into my existing life, rather than having to build my life around the course. These units allowed me to do that.

These comments also provide an insight into the learning environment facing this cohort of ECU students. Invariable security students are already practitioners in the field and this makes for an ideal opportunity for the collaboratively constructing knowledge. As Moore and Brooks (2000) 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 a preparedness to share success (p.140). In this situation, knowledge may be generated using a structured and unstructured learning interactions using Blackboard's communications facilities.

Overall, there was a favourable response to delivering the Physical Security unit online. Student's feedback is already being used to modify the courseware as part of ECU's quality initiatives. Areas for improvement were also identified, such as structured online discussions and extended use of Blackboard features. Procedures derived from ECU's Online Quality Guidelines have been incorporated into product reviews and the first offerings of the units. Analysis of regularly collected findings is being used formatively to both revise existing materials and approaches, and to inform the design of new units. More data and feedback is needed before trends can be ascertained.

Conclusion

The ECU Security Science programme is acknowledged as a high quality programme by government and industry both within Australia and in the international context. The Graduate/Executive Certificate in Security Management course 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 activities. The field of security, in addition to the subject/professional knowledge, embraces a large number of generic skills preparing students for a variety of careers in government agencies, social services and industry. The knowledge domains to be addressed by each component of the Graduate/Executive Certificate in Security Management have complied with accreditation requirements for core areas of study. The course has provided 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 of the unit is on best practice through reducing the risk of asset loss from high threat situations.

Australian Universities with offshore teaching programmes can gain 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 Science 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. Early signs indicate a positive students experience with learning materials delivered using Blackboard.

References

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

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

Herrington, A., Herrington, J., Oliver, R., Stoney, S. & Willis, J. (2001). Quality guidelines for online courses: The development of an instrument to audit online units. In (G. Kennedy, M. Keppell, C. McNaught & T. Petrovic (Eds.) *Meeting at the crossroads: Proceedings of ASCILITE 2001* (pp. 263-270). Melbourne: The University of Melbourne.

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

Hosie, P. & Mazzarol, T. (1999). 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.

Mazzarol, T. & Hosie, P. (1996) Exporting Australian higher education: Future strategies in a maturing market, *Quality Assurance in Education*, 3(3): 37-50.

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.

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

Moore, A. B. & Brooks, R. (2000). Learning communities and community development: Describing the process. Learning Communities: International Journal of Adult and Vocational Learning, Issue No.1(Nov), 1-15.

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.

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.