Internet Security Management: A Joint Postgraduate Curriculum Design

Helen Armstrong
Nimal Jayaratna
School of Information Systems
Curtin University of Technology
GPO Box U1987, Perth
Western Australia 6845
H.Armstrong@curtin.edu.au N.Jayaratna@curtin.edu.au

ABSTRACT

This paper presents the structure and content of a series of a postgraduate curriculum in Internet Security Management developed and presented jointly by the Schools of Information Systems and Computer Science at Curtin University of Technology in Western Australia. The integration of generic skills (including problem solving, risk and project management, change management and research methods) with specialist security knowledge and practical project courses is also discussed.

Keywords: Internet security, security management, information security education.

1. INTRODUCTION

Over the past few years the rise in cybercrime has brought computer security concerns to the forefront. Organisations are beginning to realise that the belief that "it won't happen to us" is a myth. The demand for educational programs in Internet and web studies has risen, and governments around the world are encouraging the development of Internet and electronic commerce security courses at both undergraduate and postgraduate levels.

A media release in February 2001 by Senator the Hon Richard Alston, Minister for Communications, Information Technology and the Arts (NOIE, 2001a), states that Information Security is a major national priority in Australia. In addition, the draft Report on E-Security R&D in Australia released by the National Office for the Information Economy states that "The [Australian] Government has a clear role to protect information infrastructure, which is critical to national security, and protect the public from criminal or malicious activity occurring through electronic mediums, primarily the Internet." (NOIE, 2001b).

In response to these national priorities and the needs of industry and government, Curtin University has designed a postgraduate program in Internet Security Management. The program is run jointly by the School of Computer Science and the School of Information Systems, and attempts to balance the technical, conceptual and human skills required to meet the above challenge.

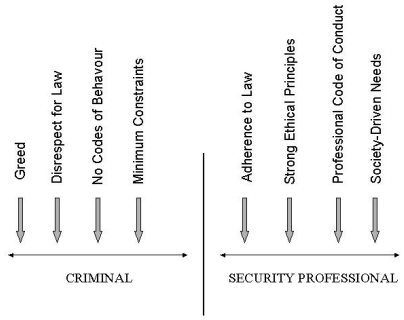
2. RATIONALE

A number of factors have contributed to the design of this new curriculum in Internet Security Management. The marked growth in computer networks, global communications, Internet access and electronic commerce has resulted in an increase in the demand for security professionals. Skills and knowledge in security are increasingly sought by both public and private organizations in order to protect their systems and data from cybercrime.

Statutory requirements necessitate that business management be more accountable for their actions. Legal requirements relating to duty-of-care are ensuring that security issues be addressed more comprehensively than in the past. The complex and unpredictable nature of computer systems affects the amount of trust we can place in these systems. For a networked information system to be trustworthy it must do what it is required to do, no more and no less, despite disruption from the environment, operator and human errors, and attacks by hostile parties (Schneider 1999). Protective mechanisms are required to ensure that networked information systems can achieve a trusted state.

Many consider information security to be a technical issue. However, the mind-sets that generate security problems and criminal activities are not necessarily technical in nature. The guiding forces that act on a security professional are adherence to law, professional code of conduct, commitment to ethical principles, care

Figure 1: Guiding Forces in Security Domain



code of conduct, commitment to ethical principles, care and respect for individuals and society. On the other hand, the forces that act on a criminal are greed, detection, prevention and recovery strategies disrespect for law, total freedom with minimum constraints and no codes of behavior (see Figure 1). Security personnel need to think, but not act, like criminals if they are to develop effective detection, prevention and recovery strategies

Information security professionals need to deal with people, both criminals and non-criminals, in every aspect of operations. They need to learn to manage relationships with people very sensitively if they are to discover criminal activity. Their judgment has to be "correct" if they are to receive co-operation as well as detect security breaches. All these point to skills in investigative and interrogative areas, effective communication and people management. This means a related and yet different set of skills is required.

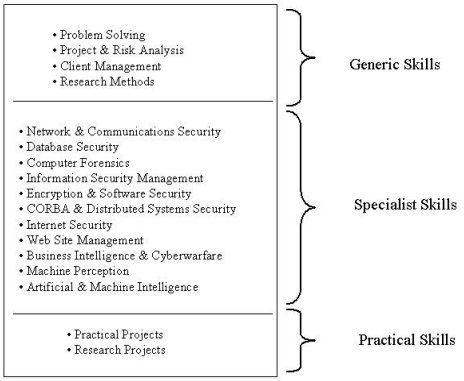
Curtin University has a commitment to society to provide graduates with skills and knowledge in security, including ethics. Figure 2 illustrates the three main areas of skills in the new program structure – generic skills, specialist security skills and practical skills. The generic component is extremely significant for the development of skills that will have a high conceptual focus. The generic components of the program are Problem Solving, Project and Risk Management, Change Management and Research Methods.

An information security professional is primarily a problem solver. Therefore there is a need to develop their generic problem solving skills. Using a range of different problem scenarios and conceptualising processes, the professional's skills need to be developed to undertake problem formulation, solution design and implementation as well as subsequent evaluation. Another set of requirements includes concepts for developing critical thinking, creative thinking and innovative thinking. The latter requires the information security professional to undertake paradigm shifts in their reasoning roles.

Another generic skill that is required by the information security professional is the ability to handle communication and interpersonal issues. Not only do they need to develop skills in people management but also to learn to manage change. Change involves multi-dimensions of mind-sets, procedures, policies, behavior and communication.

The third generic skill set is in the area of project and risk management. Most security improvements or implementations involve resources (financial and human) and therefore efficient resource management skills are needed to achieve effective outcomes. Risk analysis enables the classification of critical and

Figure 2: Structure includes generic, specialist and practical skills



valuable resources, and identification of vulnerabilities. Risk management concepts assist information security professionals to determine the balance between the costs and implications of taking action, versus non-action, and aids in the decision-making for the most appropriate solution selection.

The last of the generic skills are in research methods. Since security is not a static area there will always be social, political, technical, economic and behavioural challenges to overcome. The mind-set of information security professionals needs to be developed to enable them to search out information relevant to topics they confront, identify channels most relevant to the areas under investigation, determine how one validates the findings and discover the ways they can keep themselves informed and contribute to knowledge in the information security area.

Since the purpose of this educational program is to develop expertise and skills in information security in an Internet environment, the postgraduate students also need to develop knowledge and skills in the technical area in which they will apply these generic skills.

The dynamic nature of the business environment requires electronic storage and transmission of vast

amounts of data. To secure this data, and the infrastructure on which it resides and moves, requires specific technical skills in the security of networks and communications, databases, operating systems, Internet, electronic commerce, computer crime and cyberwarfare, and computer forensics (see Figure 2).

The final category of skills is practical. Information security is a practical discipline. The solutions that are constructed using generic and specialist skills need to be effective in practice. They also have to be integrated in practice. The third stage of the education program is to ensure that students are able to integrate their knowledge and achieve effective results within a practical domain. To achieve this aim students will work on practical case studies developed jointly with industry. Outside organizations will be involved to create realistic settings for which students will be required to design secure networks and environments and test them. Students will then be required to write up a project report showing not only how they understood the construction and implementation of solutions but also what abstract lessons they learned from the project.

The latter abstract learning is more advanced than Bloom's (1956) taxonomy and Kolb's (1984) experiential learning. The learning theory is more aligned to the "double loop" learning model (Argyris 1982, Argyris & Schon 1974), however the vertical abstraction of the notions, concepts, lessons will be advanced using the NIMSAD framework (Jayaratna, 1994). This framework requires evaluation of lessons along three dimensions: the situation; use of tools, techniques, models, concepts, methods and methodology; as well as critical self-reflection using "mental construct" elements at three time periods – before, during and after intervention. The most important abstraction is the discovery of self and the assessment of further learning needs.

The program thus aims to develop postgraduates with the conceptual and intellectual power to adapt their acquired knowledge and skills into their future working environments. The design of the program structure incorporates a generic component, specialist component on security and a practical component in which the previously learned material are brought together as instruments for guiding practice (see Figure 2).

3. STRUCTURE OF THE PROGRAM

The series of Internet Security Management (ISM) programs are offered at three postgraduate levels, postgraduate diploma, professional masters, and masters by coursework (see Table 1).

All courses within the program require a Bachelor degree in a computing related discipline as an entry requirement. Students with a degree in a non-computing discipline are required to complete a graduate certificate or graduate diploma in a computing related field in order to gain entry.

Table 1: Offerings within the Internet Security Management program

Program	Credits	Duration (Full-time)
Postgraduate Diploma in ISM	200	1 year
Master of ISM	300	1.5 years
Master of Commerce (ISM)	400	2 years

The program consists of three articulated degrees - a postgraduate diploma in Internet Security management, a professional Masters of Internet Security Management, and a Master of Commerce (Internet Security Management). The structure and content of the three programs is illustrated in Appendix A.

3.1 Postgraduate Diploma in Internet Security Management

This program is designed for students with a degree in a computing-related discipline who wish to enhance skills and knowledge in the design and management of Internet security and electronic commerce in business organisations. The program consists of eight courses of study each carrying 25 credits, totalling 200 credit points. The program can be seen in the first column in Appendix A; and the courses studied include project and risk management, change management, information security management, network and communications security, encryption and software security, plus two optional courses chosen from those listed. The postgraduate diploma program can be completed in one year (two semesters) of full-time study or two years of part-time study.

3.2 Master of Internet Security Management

This program is a professional masters degree containing a total of twelve courses of study. It is designed for computing professionals who wish to take leadership roles in Internet security management. Students need a computing-related degree plus a minimum of two-years relevant industry experience to enter this program.

The second column in Appendix A gives details of this program. The first eight courses of the Master of Internet Security Management are the same as the Postgraduate Diploma program. The core courses included in this program are project and risk management, information security management, problem solving, change management, network and communications security, encryption and software security, database security, computer forensics, distributed computing security, plus a double course security project or two optional courses chosen from the list in Appendix A. This professional masters program can be completed in eighteen months (three semesters) of full-time study or three years of part-time study.

3.3 Master of Commerce (Internet Security Management)

This program is designed for students who wish to continue their studies in the Internet security management field to gain further knowledge and skills in managing Internet security and electronic commerce environments. Students do not need relevant industry experience to undertake this program. The total program is 200 credit points containing a mix of eight advanced topics and research courses. To enter the program students must obtain a minimum 70% average in the Postgraduate Diploma program. The core and optional courses are listed in the final column in Appendix A. Students must complete a substantial research project, to the value of 100 points, equivalent to four courses. This project is written up as a research dissertation and published by the university, thus satisfying the entrance requirements for the PhD program. The Master of Commerce (ISM) program has a duration of one year (two semesters) of full-time study or two years of part-time study.

The concentration of this new program is Internet security management. The focus on 'Internet security' rather than 'information security' is a reflection of the emphasis on electronic networked information environments rather than physical security of information and secure building design (see Appendix B for detailed syllabus).

4. CONTENT OF COURSES

The topics covered in the three areas of skills and knowledge - generic, specialist and practical, are shown in Appendix B. Generic skills courses will provide students with the skills required to think critically, abstract and solve problems, undertake assessment of risks, manage projects, present various research methods through which the individual can pursue and further enhance and consolidate their knowledge, and provide skills in communications and management of the technology and people. The generic skills courses are problem solving, project and risk management, change management, and research methods (see Appendix B).

Specialist skills courses cover the security and technical content of the program. These include Internet structure, network structure and management, network and distributed computing security, communications security, software security, security strategy and management, Java and XML programming, computer forensics, encryption, database security, electronic commerce security, cyberwarfare, artificial intelligence and machine perception. The far right column in Appendix B indicates the School owning and teaching the course.

Project courses are research projects conducted jointly with industry. They aim to apply generic skills, together with technical and security knowledge and skills, in order to produce a tangible outcome of a practical nature and to add to the body of knowledge. This integration will be at both a conceptual and practical level and be guided by systems thinking.

5. COLLABORATION

There are many advantages and challenges in a joint program of this nature. This project has required the commitment of both schools to the time and resources required to design, develop and run these programs. The content has been based upon a shared understanding that an Internet Security Management professional needs to be holistic in approach, requiring generic, technical and practical skills.

Recognition of each other's strengths and expertise has emerged from the curriculum design process. Agreement on the technical and management content has proven to be a challenge, particularly with regard to pre-requisite knowledge for the technical areas and sequencing of the courses. Fortunately, the two schools currently work fairly closely together, recognizing duplications in courses, and allowing students to undertake optional courses in the other school.

Funding of staff and teaching resources within a university is a complicated matter. Sharing staff and resources across two different schools in different faculties creates complications. In order to work within the restricted University regulations, the two schools have agreed to share the teaching equally. Units offered by each school utilise resources from that school. The new program has raised the requirement within both schools for specialised laboratories to carry out practical work and it has been necessary to hire appropriate laboratories from other schools within Curtin University. The School of Information Systems will administer the new program as the infrastructure and systems to handle the required administration are already in place for other joint programs.

The university requires the overall program design to be approved by both Schools before being presented to the university curriculum committees and Senate for final approval. The two schools have held numerous meetings to design the structure of the programs, define the required content, develop a logical sequence, plan semester offerings and resolve problems relating to the overlap of content and prerequisite knowledge.

6. COMPARISON WITH SIMILAR PROGRAMS

Many Computer Science and Information Systems programs at other universities include security and cryptography courses (for a list see http://avirubin.com/courses.html) but only a small number have curricula dedicated to information security or Internet-related security. Appendix C gives details of a sample of security-related Masters level programs at other universities.

The content of the programs investigated was quite diverse. Programs appear to focus on security management, risk management, law and crime,

cryptography, network security, electronic commerce security, computer forensics or information warfare. Many of the programs investigated concentrated on information or computer security, particularly the technical aspects. In these programs courses in network security, cryptography, electronic commerce security and security management seem common inclusions. For instance, the Master in Computer Science at James Mason University appears to be quite technical in focus with a concentration on network security and cryptography (JMU, 2002) to the exclusion of courses on electronic commerce security, risk and security management. Conversely, the Masters in Information Technology Security offered by the University of Westminster (WMIN, 2002) appears to place less emphasis on the technical security areas.

Very few universities offer courses in computer forensics. This could be because it is resource hungry and requires specialist expertise to teach. However, Cranfield University (2002) offers a course with a specialization in Forensic Computing, incorporating courses in electronic crime, law and courtroom skills, investigations and several forensic areas. As cybercrime continues to rise it seems logical that demand for knowledge and experience in computer forensics will rise, particularly in relation to networks and the Internet.

The study of crime appears frequently, however the law and legal issues appears in only some of the programs studied. An understanding of the law from a local as well as international perspective should be an integral part of any program on security, particularly in global networked environments.

Considerations of risk appear as a separate course in only a few programs, although the study of risk is implied in many other courses included, such as assurance and security issues. Database security was found in only a small number of programs. This was surprising, as the majority of larger computer systems and web sites utilise database management systems.

Many of the programs studied contain a project or dissertation course. Surprisingly, several programs include project or dissertation courses but no research methods or project preparation courses. None of the courses investigated appear to offer studies in the wider generic skill-set of conceptual and creative thinking, problem solving or change management.

The entry requirements for the programs investigated ranged from a bachelor degree in any discipline to a first or second class honours degree in computing. It would seem obvious that knowledge of computing would be an advantage, particularly when faced with the technical aspects of security. The duration was one year in a full-time study mode, or two years part-time. A small number of programs had a duration of 1.5 years full-time or three years part-time. However, the program duration cannot be viewed in isolation from the entrance requirements, as several programs of one year duration had an entry level of a honours degree.

The new Internet Security Management programs designed by Curtin University appear consistent in duration and entry requirements to programs offered by other universities. The technical content also appears to be similar, particularly in the areas of network security, electronic commerce security and cryptography. The uniqueness of the proposed programs at Curtin University is the holistic design of the program to integrate technical, management and practical security skills together with generic skills in problem solving and change management. The joint venture between the Schools of Information Systems and Computer Science has enabled a unique integration of security skills and knowledge across the disciplines.

7. CONCLUSION

The design of the new programs in Internet Security Management is complete, and commencement is planned at the beginning of 2003. The programs described above have attempted to meet the need for security graduates who have the ability to conceptualise, are problem solvers, are technically proficient, and have practical experience in applying the security knowledge and skills in an information security and Internet security context. The program also provides three levels of qualification in the Internet security management field with direct articulation between the courses.

The mix of generic skills, and specialist knowledge and skills, and practical project courses are planned to develop a well-rounded graduate, one who has the ability to solve problems in the Internet security arena. The practical application of theory via the project courses will assist students to consolidate their learning by actually doing and then reflecting upon that learning process. Students will also gain confidence in their ability to apply knowledge and skills to problem situations.

8. REFERENCES

Argyris, C. [1982], Reasoning, Learning and Action, Jossey-Bass, USA

Argyris, C. and D. Schon [1974], Theory in Practice: Increasing Professional Effectiveness, Jossey-Bass, USA

Bloom B, M. Englehard, E. Frost, W. Hill & D. Krathwohl [1956], Taxonomy of Educational Objectives: The classification of Educational Goals: Handbook 1, Cognitive Domain, Longmans, New York

Cranfield University [2002], Forensic Computing, http://barrington.rmcs.cranfield.ac.uk/directories/postgrad/445868?view=www) (accessed 29/7/2002)

GLAM [2000] MSc Information Security and Computer Crime, Glamorgan University http://www3.glam.ac.uk/Prospectus/view.php3?ID=849&sfrom=easy&dosommat=string&year=2002 (accessed 29/7/2002)

JMU [2002] Infosec Program, James Mason University,http://www.infosec.jmu.edu/program/html/program.html (accessed 29/7/2002)
Jayaratna, N., [1994], Understanding and Evaluating Methodologies, McGraw Hill, Maidenhead.
Kolb, D.A. [1984], Experiential Learning: Experiences as a Source of Learning and Development, Prentice-Hall Inc, Englewood Cliffs, New Jersey
LE [2002] Postgraduate Prospectus, MSc in Security and Risk Management, Leicester University, http://www.le.ac.uk/cgi-bin/tab_int/usr/netscape/suitespot/docs/ua/hd/pgprospectus/courses/courses.txt?operation=retrieve&primary=m900d1 (accessed 29/7/2002)
NOIE [2001a] Information Security – A Major Priority, Media release from the National Office for the Information Economy, Available WWW http://www.noie.gov.au/publications/media_releases/feb2001/infosecurity.htm
NOIE [2001b] Report on E-Security R&D in Australia: An Initial Assessment, National Office for the Information Economy, Canberra, Australia, June
RHUL [2000] MSc in Secure Electronic Commerce, Royal Holloway University of London, http://www.isg.rhul.ac.uk/msc/sec.html
Schneider Fred B. [1999] Trust in Cyberspace, National Academy Press, Washington DC, USA
WMIN [2002] MSc in Information Technology Security, Westminster University, http://www.wmin.ac.uk/solape/item.asp?ID=3888&wp=pgs (accessed 29/7/2002)

AUTHOR BIOGRAPHIES

Helen Armstrong (B.Com DipEd, Dip IS, PhD). Helen co-ordinates postgraduate and undergrad-uate programs and teaches within the School of Information Systems. Helen has a keen interest in computer security, computer crime and cyberwarfare.

Nimal Jayaratna is Head of School for the School of Information Systems at Curtin University and researches in the area of information systems methodologies. He is the Chair of the British Computer Society Methodology Specialist Group

Appendix A: Structure of the Postgraduate Diploma and Masters Programs in Internet Security Management

Study Plan Full-time	Postgraduate Diploma in Internet Security Management	Master of Internet Security Management	Master of Commerce (Internet Security Management)
Year 1 Sem 1	Project & Risk Management	Project & Risk Management	Project & Risk Management
	Information Security Management	Information Security Management	Information Security Management
	Problem Solving	Problem Solving	Problem Solving
	Network & Communications Security	Network & Communications Security	Network & Communications Security
Year 1 Sem 2	Change Management	Change Management	Change Management
	Encryption & Software Security	Encryption & Software Security	Encryption & Software Security
	Optional Course	Distributed Computing Security	Distributed Computing Security
	Optional Course	Database Design & Security	Database Design & Security
Year 2 Sem 1		Computer Forensics	Computer Forensics
		Research Methods	Research Methods
		Plus Either: Security Project (50 credits = 2 courses) or 2 Optional courses	2 Optional Courses
Year 2 Sem 2			Security Project (100 credits = 4 courses)
	Optional Courses:	**Optional Courses:**	**Optional Courses:**
	Database Design & Security	Machine Perception	Machine Perception
	Computer Forensics	Artificial & Machine Intelligence	Artificial & Machine Intelligence
	Distributed Computing Security	Networking & Mobile Communications	Networking & Mobile Communications
	Web Site Management	Internet and JAVA	Internet and JAVA
	IS Research Methods	Web Site Management	Web Site Management
		Business Intelligence & Cyberwarfare	Business Intelligence & Cyberwarfare
		XML and Electronic Commerce	XML and Electronic Commerce
		Electronic Commerce Security	Electronic Commerce Security
		Internet Law	Internet Law

Appendix B: Topics covered in Postgraduate Diploma and Masters courses

Course Name	Credits	Course Focus	School
Artificial & Machine Intelligence	25	Computers as security intelligence tools, LISP, list processing, pattern matching, symbolic representation, search methods, semantic nets and frames, neural networks, machine learning, constraint propagation, probabilistic reasoning, planning and problem solving paradigms	Computer Science
Business Intelligence & Cyberwarfare	25	Intelligence cycle, business intelligence models, competitive intelligence, industrial espionage, methods and tools, cyberwarfare attacks, protective mechanisms	Information Systems
Change Management	25	Behavioural aspects of change, management of change, human communications, conflict resolution	Information Systems
Computer Forensics	25	Computer architectures, Internet architecture, computer forensics technology, isolation of equipment and files, data recovery, evidence collection and data seizure, duplication and preservation of digital evidence, computer image verification and authentication, discovery of evidence, reconstruction of past events, encryption and forensics, national & international legal issues	Information Systems
Database Design & Security	25	Database models, normalisation, physical storage, record access paths, design and performance evaluation, database integrity, consistency, inference, security controls, concurrency, transaction schedules and protocols, recovery techniques, encryption in databases, distributed databases, database driven web-sites, trusted front-ends	Computer Science
Distributed Computing Security	25	Design of distributed computing, distributed computing models, UML, Java, CORBA, file and transaction handling, security design of distributed environments	Computer Science
Electronic Commerce Security	25	EC risks, EC infrastructure security, Encryption in EC, privacy, secure payments, role of audit, secure messaging, VPNs, non-repudiation, PKI, certification policies	Information Systems
Encryption & Software Security	25	Symmetric and asymmetric key distribution, protocols and key management, cryptanalysis and breaking of codes, international standards and laws, digital signatures and certificates, SHA secure hash algorithm, firewalls, IPSec, DNSSec, encryption in biometrics and smartcards	Computer Science
Information Security Management	25	Computer crime, security risk analysis, physical security, control and remote and local access, administrative controls, network security management, biometrics and authentication, measurement of potential loss, security audits, contingency planning	Information Systems
Internet and JAVA	25	Internet architecture, distributed application development, Internet-based mobile agents, automating the Internet, coordinating distributed components over the Internet, security issues, automated Web applications, Web programming, supercomputing on the Web	Computer Science
Internet Law	25	The advent of electronic media has raised critical issues in terms of both national and international law. Exploration of fundamental issues with an emphasis on their application in an electronic environment	Business Law
IS Research Methods	25	Philosophy of research, major research methods and their applicability, including scientific method, phenomenology, ethnomethodology, ethnography, grounded theory, action research, hermeneutics, experimental design, surveys and questionnaires, content analysis, symbolic interactionism, multi-methods and triangulation.	Information Systems
Machine Perception	25	Machine vision, speech recognition, image data capture & processing, data compression, video/image processing, speech processing, syntactic and statistical pattern recognition, neural networks, machine learning, data	Computer Science

		mining, application to security products and biometrics	
Network & Communications Security	25	TCP/IP, Netbios and RTS, distributed programming with remote procedure calls, network management protocols (SNMP and CMIP), network statistical analysis and debugging, client-server architectures, network installation and maintenance, routing, managing network security	Computer Science
Networking & Mobile Communications	25	Advances in usage and application of computer networks. Programming and adaptation of active networks. Issues in mobile computing, multimedia transmission and QOS issues in wired and wireless networks. Internet-based solutions to distributed application problems. Security issues. A view to the future of computer networks.	Computer Science
Problem Solving	25	Nature of problem structuring, problem situation improvement, positivist and interpretivist views of organisational problem solving, uncertainty, multiple and conflicting objectives in problem solving, detailed examination of one or more 'soft' methodologies	Information Systems
Project & Risk Management	25	Project management methods, starting up a project, establishing the project management team, quality, risk assessment, risk management, project controls, managing product delivery, managing stage boundaries, closing a project	Information Systems
Security Project	50	Practical project in network security design, building and testing. White-hat, red-hat and black-hat network attacks, real time network reconfiguration , network forensics and evidence collection	Computer Science & Information Systems
Security Project	100	Individually supervised research project on a security topic	Computer Science & Information Systems
Web Site Management	25	Webmaster functions - Internet strategy, information architecture formulation, project and operations management, quality assurance. It also reviews Web site evolution cycle, Web site issues - standards vs innovation, static vs active pages, content vs technology, intranet vs internet, security vs open access and integration issues.	Information Systems
XML and Electronic Commerce	25	XML programming, future trends and issues in Electronic Commerce including societal impacts, technnology trends, organisational and work place impacts.	Information Systems

Appendix C: Similar Programs at other Universities

University	Degree Name	Duration	Entrance	Security Contents
James Madison University (JMU, 2002)	MSc in Computer Science	1 year via Internet	U/G Degree	Network security, Cryptography, Assurance, Advanced Network Security, Audit & Secure Operations, Distributed Computing & Security
University of Glamorgan (GLAM, 2002)	MSc in Information Security & Computer Crime	1 year full-time	U/G Degree	Security Management, Project Management & Research Methods, Network & Distributed Systems Security, Cryptography & E-commerce, Computer Law & Criminology, Computer Forensics
Royal Holloway University of London (RHUL, 2002)	MSc in Secure Electronic Commerce	1 year full-time	U/G Degree	E-commerce Business & Security Issues, Cryptography, Secure E-Commerce infrastructure & Standards, Legal aspects of E-Commerce, Secure E-Commerce technology, Standards & Evaluation Criteria, Advanced Cryptography, Database Security, Computer Crime, Project
University of Westminster (WMIN, 2002)	MSc in Information Technology Security	1 year full-time 2 years part-time	Honours degree	Security Awareness, Threats, Countermeasures, Standards & Procedures, Legal & Ethical Aspects, Risk Analysis, Business Needs, Policy & Planning, Security Analysis, Post-incident Reviews, Security Management, Computer Forensics, Security, Project Module
University of Leicester (LE, 2000)	MSc in Security & Risk Management	1 year full-time 2 years part-time	Honours degree	Intro to Security Management, Crime and the Workplace, Research Methods in Security & Risk Management, Managing Risk and Security, Applied Crime Management, Management, Organisations & Security, Dissertation
Cranfield University (Cranfield University, 2002)	MSc in Forensic Computing	3 years part-time	Honours degree	Forensic Computing, Systems Programming, Law & Courtroom Skills, Corporate Security, E-Crime, Internet investigations, Forensic Networks, Forensic Internet

Information Systems & Computing
Academic Professionals

STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the Journal of Information Systems Education have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

ISSN 1055-3096