Internet Security Management –a New Postgraduate Program in Australia

Helen Armstrong and Nimal Jayaratna

School of Information Systems
Curtin University
GPO Box U1987
Perth, Western Australia 6845

School of Information Systems
Curtin University
GPO Box U1987
Perth, Western Australia 6845

Phone: +61-8-9266 7017
Fax: +61-8-9266 3076
Email: H.Armstrong@curtin.edu.au

+61-8-9266 7027
+61-8-9266 3076
N.Jayaratna@curtin.edu.au

Abstract

Many view the solutions to information assurance with an increasingly technical focus, however the mindsets and actions that generate security problems are not solely technical in nature. Security specialists need strong conceptual skills in order to think in a number of different ways. Postgraduate programs in the information assurance arena need to carefully balance the technical, conceptual and human skills. This paper is a brief overview of a postgraduate program in Internet Security Management currently being developed at Curtin University in Perth, Western Australia. The course is jointly offered by the Schools of Computer Science and Information Systems and incorporates generic, technical and management skills. This paper explains the philosophy and structure for the Masters of Internet Security Management.

Internet Security Management –a New Postgraduate Program in Australia

Introduction

As business moves to a more global marketplace and communications facilities become more sophisticated, the need for formal education in the area of information assurance and information security management is apparent. Security is also a contemporary issue with the rate of computer and web-based crime rising and the increased fear of cyberterrorism in the wake of September 11. With the complexity of technology and computer communications rising, a combination of what appear to be seemingly unrelated vulnerabilities can place a company in great jeopardy (Robinson, 2000). Any individual specialising in the area of information assurance requires skills in detection, prevention and recovery. Invariably recovery is a high cost item, and with sufficient prevention and detection measures in place, this cost can be minimised.

Many view the solutions to information assurance with an increasingly technical focus, however the mindsets and actions that generate security problems are not solely technical in nature. Security specialists need strong conceptual skills in order to think in a number of different ways, and to think like a criminal. As they deal with people in all three of the domains of detection, prevention and recovery, security specialists also need to be able to manage human relationships with strong communication and examination (investigative and interrogative) skills. Postgraduate programs in the information assurance arena need to carefully balance the technical, conceptual and human skills.

This paper is a brief overview of a postgraduate program in Internet Security Management currently being developed at Curtin University in Perth, Western Australia. The course is jointly offered by the Schools of Computer Science and Information Systems and incorporates generic, technical and management skills. This paper explains the philosophy and structure for the Masters of Internet Security Management.

Information Assurance Education in Australia

Similar to the USA the Australian Federal Government has been attempting to raise the profile of information security and protection of critical infrastructure. In his Opening Address at the Second World Conference on Information Security Education in July 2001, the Hon Daryl Williams MP QC, Attorney General of Australia stated that cyberterrorism is an emerging threat for which we must be prepared. It is vital that the National Information Infrastructure be protected from viruses, hackers, denial of service attacks and information warfare (ADG, 2001). An important part of the Attorney General's strategy is forming international links with other countries actively pursuing critical infrastructure protection for training and research and development purposes.

The Report on Protecting Australia's National Information Infrastructure (AGD, 1998) specifies there is a low level of awareness generally amongst both government and industry about the type of level of threats to computer networks. The report goes on to say that those persons or organisations who may pose a threat to information security and the national information infrastructure include individuals who cause

unintentional disruption, hackers, disgruntled employees or contractors, criminals, those engaged in commercial espionage, issue motivated groups, terrorists and foreign states.

A media release in February 2001 by Senator the Hon Richard Alston, Minister for Communications, Information Technology and the Arts (NOIE, 2001a), states Information Security is a major priority. In addition, the draft Report on E-Security R&D in Australia released by the National Office for the Information Economy (NOIE) in June 2001 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). The report goes on to say that maintaining a critical mass of e-security R&D in Australia is essential to achieving the Government's aim to ensure Australia is a global supplier of e-security products and services.

With the view of providing postgraduate students with skills and knowledge in information security to meet the needs of industry and government, Curtin University has designed a Master of Internet Security Management. The course 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.

New Masters in Context

Students who graduate from Masters and Postgraduate Diploma courses in Internet Security Management will be problem solvers in the first instance in the security arena, operating at a high level of abstraction and be able to translate this into practice (Jayaratna, 1991). During their postgraduate studies, students will develop specific technical skills and be able to apply these within a generic set of skills also acquired during the course. The program includes a project component, the focus of which will be the 'learning from the doing' to ensure students' understanding and the relevance of knowledge gained. Hence students will acquire critical thinking, management as well as technical knowledge and skills.

Three areas of skills and knowledge are proposed for the Internet Security Management area, as in all postgraduate offerings within the School of Information Systems – generic, specialist and project.

Generic skills units 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 (Jayaratna, 1994; Schien, 1987, 1988).

Specialist skills units cover the security and technical content of the course including Internet structure, network structure and management, network security, communications security, security strategy and management, computer forensics, encryption and so forth.

Project units are research projects conducted jointly with industry that aim to apply generic skills with technical and security knowledge and skills, to produce a tangible outcome of a practical nature and add to the body of knowledge. This integration will have to be at a conceptual and practical level and be guided by systems thinking. A significant focus in the project will be the student's ability to abstract lessons using methodologies and frameworks (Argyris & Schön, 1984; Schön, 1983; Schien 1993a and 1993b).

The project unit incorporate features of action in the learning process, an approach that has been espoused for more than three decades, including experiential learning (Kolb, 1984) and action learning and action research (Revans, 1999), necessitating planning and knowledge gathering, application or action, and reflection. Weinstein (1999:3) describes action learning as 'a way of learning from our actions and from what happens to us, and around us, by taking the time to question, understand and reflect, to gain insights, and consider how to act in future'. The use of project units will assist students to consolidate learning and gain confidence in their ability to apply knowledge and skills to problem situations (Argyris, 1980; Argyris et al., 1985).

The human brain uses five lanes to process information and store it in memory (Sprenger, 1999): semantic (only words), episodal (contextual), procedural (motor skills), automatic (stimuli-response) and emotional memory lanes. Retrieved memories are the only evidence we have of learning and the memory lanes provide the mechanism to access the data. The more memory lanes used for storage of an event or information, the more powerful the learning will be. The practice of conceptualising, evaluating and physically experiencing practical application utilises several memory lanes, thus consolidating the memories and learning process.

Students must have completed the generic unit on research methods before embarking upon their security project unit. The projects will be supervised by academic staff with an interest or expertise in the chosen area, thereby increasing opportunities for joint research with industry partners and research publications.

Overview of Masters Course Structure

The Masters of Internet Security Management program consists of two stages, the Postgraduate Diploma and Masters stages as illustrated in Figure 1.

The Postgraduate Diploma stage consists of eight units of study totalling 200 credit points. Students must complete three of the four generic skills units and five specialist units. The specialist units cover areas such as the security of Internet and network architecture, computer communications security, electronic commerce security, database security, encryption technologies, computer and Internet crime, and information assurance management.

The Masters stage consists of four units of study totalling a further 100 points. Students must complete the remaining generic skills unit and a unit in computer forensics. A research project with industry carrying 50 credits, equivalent to two other units, is required to complete the masters. A dissertation or thesis must be produced at the conclusion of the project.

Program Stage	Course Content	Credits
Postgraduate Diploma (must have completed Bachelor degree in Computing/IT)	**Generic Units** Choose three from – • Problem Solving • Risk & Project Management • Research Methods • Behavioural & Change Management **Specialist Units** Choose five from – • Network/ Internet Architecture & Security • Communications Security • Electronic Commerce Security (Introduction) • Electronic Commerce Security (Advanced) • Crime and Security Management • Database Security • Encryption Technologies • Software Security	Each Unit = 25 credits 3 x 25 = 75 5 x 25 = 125 Total 200 credits
Masters (must have completed Postgraduate Diploma)	**Generic Units** Choose remaining one from – • Problem Solving • Risk & Project Management • Research Methods • Behavioural & Change Management **Core Specialist Unit** • Computer Forensics **Core Project Unit** • Research Project (2 unit 50 credits)	1 x 25 = 25 1 x 25 = 25 2 x 25 = 50 Total 300 credits

Figure 1: Structure of the Masters in Internet Security Management

The specialist skills units are a combination of theory and practical work. Each unit has a substantial laboratory and field work component and students are expected to apply the theory they have learned. For example, students will build, attack and reconfigure networks; build, attack and reconfigure web sites and databases; perform forensic investigations on workstations and networks; develop security policies and procedures; design secure physical environments, and apply appropriate encryption technologies to industry situations. Some of the laboratory work will be conducted in conjunction with industry partners.

The entire Masters can be completed in eighteen months full-time study or three years part-time study. Upon completion of the Masters program, a student will have studied all four generic units, 6 specialist units, completed a 50 credit project unit and submitted a research report or dissertation based upon the project.

Entry Requirements

Students may enter the program with a bachelor degree (3 year undergraduate degree)

background is required for students to understand and apply the technical components of the Masters program. Students with bachelor degrees in non-computing disciplines who wish to enter the course are required to complete a Graduate Diploma in IT to gain the pre-requisite computing skills before embarking on the Masters program.

Conclusion

The Masters of Internet Security Management is a program designed to support the Australian Federal Government's push to raise the profile of information assurance education and develop a critical mass of e-security education and research within Australia's own shores. The program is unique in design offering a balance of technical, conceptual, human interaction and management skills in the information assurance education sphere. The proposed program is action based emphasising the practical application in relevant industry contexts, allowing the merging of expertise, knowledge and facilities to create a focus for security education and research activities jointly with industry.

The Masters of Internet Security Management is planned to commence in the second half of 2002, however, there is keen interest in the course already. Students are enrolling in parallel Masters courses with the intent to transfer to the new Masters when it has the University's final seal of approval.

References

ADG (1998) *Protecting Australia's National Information Infrastructure, Report of the Interdepartmental Committee on Protection of the National Information Infrastructure*, Attorney-General's Department, Canberra, Australia, December.

ADG (2001) *Security in a Borderless World*, Opening Address at the Second World Conference on Information Security Education, Western Australia, July, Available WWW http://www.law.gov.au/ministers/attorney-general/articles/borderless.html

Argyris, C., (1980), *Inner Contradictions of Rigorous Research*, Academic Press, London.

Argyris, C., Putnam, R., Smith, D., (1985), *Action Science : concepts, methods and skills for research and intervention*, Jossey-Bass, San Francisco.

Argyris, C., & Shön, D., (1978), *Organisational learning : a theory of action perspective*, Addison-Wesley, Reading.

Jayaratna, N., (1991), Systemic analysis: The Missing Link in the Systems Development Process, *Journal of Applied Systems Analysis*, vol 18

Jayaratna, N., (1994), *Understanding and Evaluating Methodologies*, McGraw Hill, Maidenhead.

Kolb D.A., (1984) *Experiential Learning: Experience as a Source of Learning and Development*, Prentice-Hall Inc, New Jersey USA

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

Revans R., (1998) *ABC of Action Learning*, Lemos & Crane, London UK

Robinson, C.A., (2000) Electronic Commerce Commands Canny Insight into Hacker Moves, *Signal*, 54 (9), pages 53-56

Schein, E. H. (1987) *Process Consultation*. Vol. 1. Reading, Addison-Wesley, MA.

Schein, E. H., (1988) *Process Consultation*. Vol. 2. Reading, Addison-Wesley, MA.

Schein, E. H. (1993a) How Can Organizations Learn Faster? The Challenge of Entering the Green Room. *Sloan Management Review*, 34, 85-92.

Schein, E. H. (1993b) On dialogue, culture, and organizational learning. *Organizational Dynamics*, Winter, 40-51.

Schön, D., (1983) *The Reflective Practitioner, How Professionals Think in Action*. Basic Books.

Sprenger, M., (1999) *Learning & Memory – The Brain in Action*, ASCD Publication, VA USA

Weinstein K., (1999) *Action Learning*, Gower, Vermont USA