Information Security Management Curriculum Development: An Australian Example

Matthew Warren and Shona Leitch
School of Information Systems, Deakin University, Burwood, Victoria, Australia

mwarren@deakin.edu.au; shona@deakin.edu.au

Abstract

The development of Information Security as a discipline has only occurred in recent years. Currently Information Security topics are widely taught at tertiary institutions but these topics are taught from a technical perspective and in other cases from a business perspective.

This paper discusses the development of a new security curriculum within Australia and how Australian tertiary institutions responded to that curriculum, the paper also puts forwards a framework that assists in curriculum development.

Keywords: Information Security, Framework, Curriculum Development and Australia.

Introduction

The development of Information Security as a discipline has only occurred in recent years. Currently Information Security topics are widely taught at tertiary institutions but these topics are taught from a technical perspective and in other cases from a business perspective. This means that the focus of Information Security can vary from a technical aspect e.g. the actual technologies involved in security to the management aspect, e.g. management polices in relation to security, and this can result in confusion and misunderstandings.

One problem that all developed countries have faced in recent times has been how to define a policy for E-Security / Information Security at a national level. In order for this policy to be effective it must also cover key issues such as security education and security research (Warren, 2003).

Historically at tertiary institutions, courses in Information Security have been offered as specialist topics, as a small part of a wider curriculum, or as programs designed just for security (Bogolea & Wijekumar, 2004). Research by key researchers (Liles & Kamali, 2006) has focused on how security can be included into a national IT Curriculum e.g. ACM SIGITE (ACM, 2008).

Within Australia there are a number of Universities, e.g., Queensland University of Technology, Edith Cowan, that offer undergraduate and postgraduate courses in Information Security. These courses can involve some aspects of management but the focus is more upon the technology aspects of security. These courses are offered from Schools or Faculties of Technology, as mentioned before this means that the courses have a very technology focus and are not usually suitable for commerce students. The ration-

ale for the development the Information Security major for commerce students was to emphases the management focus of security rather than the technology focus.

This paper will focus upon the Information Security, in particular; example of the development of a national strategic direction, examples of security education curriculum development, the development of a security curriculum framework and associated examples.

Developments of a National E-Security / Information Security Curriculum and Research Policy (Australia)

Some of the authors have identified and mapped the development of the National E-Security Curriculum within Australia (Warren, 2003). The Federal Government of Australia's National Office of the National Economy (NOIE) had been investigating the Australian E-Security situation by undertaking a number of capability projects. NOIE's role was to strengthen Australia's participation in the global Information Economy, and to focus upon key technology issues. The aim of the first NOIE project was to determine what the situation was within Australia in regards to E-Security education. The project found that the main issues were (Aeuckens, 2001):

- Demand for people with E-Security skills is expected to be strong over the few years;
- Recruitment of personnel with E-Security skills is difficult compared to other IT&T skills.

This project also identified some key issues that related to Australian organisations and the impact of E-Security, these key issues were (Aeuckens, 2001):

1. Demand is rising. As E-Security becomes an integral business issue, demand for skilled personnel is growing within Australia;
2. Recruitment of people with the right skill sets is difficult. The greatest difficulty is in recruiting people with well-rounded security and risk management skills (likely to include technical and business skills);
3. E-Security is not just an issue for security personnel. All IT personnel should have an awareness of E-Security issues and its place in a business environment;
4. Limited Graduate programs. Many organisations recruited new IT graduates. Graduates did not generally have any specific understanding of security, therefore it was necessary for them to undergo further training;
5. Education and training opportunities in E-Security are not widely available. The minimum qualification demanded by employers is generally at the Bachelor level but these lack security content.

A further NOIE investigation was into E-Security research and its development within Australia. This NOIE project found it was essential to ensure the long-term future of E-Security research for a number of reasons (King, 2001) and to ensure that Australia's E-Security R&D capability was developed. NOIE had defined within its National E-Security strategy two major key areas which were important for the future of Australia, these were:

- E-Security Teaching – ensuring that E-Security skills are taught at Australian Universities to all students. Ensuring there is co-operation between Australian Universities and industry to teach and develop courses;
- E-Security R&D – ensuring that E-Security R&D is considered important area for Australia's future R&D national strategy.

Events outside of Australia caused a major impact, the bombing of the World Trade Center (September 11, 2001) and the Bali bombing (October 12, 2002) had a direct impact upon Australian national policy (as it did for many other countries) such as the announcement in the Australian Federal budget (2001-02) that A$400 million would be allocated over four years for defence purposes (Scott, 2001). This change in budget allocation obviously impacted the budgets of other government departments and others involved in security were therefore reduced. In 2002 the structure and role of NOIE was changed, the area of IT industry policy and its development was removed from its portfolio, this had in impact upon the role of NOIE (Cant, 2002). Following the changes within NOIE in 2002, "The amended National E-Security strategy" was cut back to only one area of the initial National E-Security strategy, which was:

- The feasibility of an industry-backed E-Security professional certification scheme should be further investigated, including the potential applicability of the internationally available schemes to Australian industry and government needs.

On 8 April 2004, the Australian Government Information Management Office was established, replacing the NOIE and merging many of its key duties. On 22 October 2004 the Prime Minister, John Howard, announced that The Australian Government Information Management Office will be incorporated within the Department of Finance and Administration, also at this time some functions of the former NOIE relating to broader policy, research and programs have been transferred to the Office for the Information Economy in the Department of Communications, Information Technology and the Arts (Howard, 2004).

Following the events of 2004, the concept of the development of National E-Security Curriculum was put on hold until 2006. In 2006 a new Review of the E-Security National Agenda based upon the 2001 review was announced (Coonan, 2006), but an election in 2007 resulted in a new Australian Federal government.

On 2 July 2008, the Australian Federal Government announced a review into the Government's E-Security policy, programs and capabilities. The purpose of the review is to develop a new Australian Government E-Security Framework in order to create a secure and trusted electronic environment for both public and private sectors (E-security review, 2008a). An interesting feature is that in the terms of references of the review there was no mention of education or the development of an E-Security Curriculum Development (E-security review, 200b).

Since 2001, the impact of the attempted development of a National Australian E-Security Curriculum Policy has resulted in Universities and professional bodies developing their own courses independently, this has meant there has been a lack of cohesion and a lack of harmonisation between the different providers. Research has been undertaken in this area to try and resolve this situation (Tate et al, 2007).

Security Curriculum Background

The way that Australian Universities has responded to the development of the E-Security Curriculum is indicative in the courses that have been developed. Focussing on focus on Master level postgraduate courses will highlight how some Australian Universities have developed their courses.

Standalone Security Course

These are dedicated Masters courses that relate to a broad coverage of Information Security areas. An example of this is the Master of Information Systems Security at Charles Sturt University. The areas covered by the courses include (Charles Sturt University, 2008):

Core Subjects

- Topics in IT Ethics
- Network Security
- Information Security
- IT Risk Management
- Interconnecting Network Devices
- Virtual Private Network and Firewall Management
- Designing a Secure Distributed Network
- Operating System Essentials
- Supporting a Network Infrastructure
- Network Security Fundamentals

Elective Subjects

- Principles of Database Management
- Systems Development Project Management
- Network and Security Administration
- IT Management Issues

Niche Security Course

These are unique Masters courses that focus just on one area of security. Edith Cowan University offers a Masters of Digital Forensics that focuses purely upon the security area of Computer Forensics. The areas covered by the course include (Edith Cowan University, 2008):

Core Subjects

- Computer Security
- Network Security Fundamentals
- Introductory Computer Forensics
- Wireless Security
- Wireless and Mobile Computing Security
- Computer Forensics
- Network Forensics
- Special Security Topic
- Forensic Investigation and Evidence Presentation
- Mobile Forensics

Embedded Security Course

These are traditional Masters of Information Technology (IT) courses that have an optional security stream. Queensland University of Technology offers a Masters of IT that has a Security stream that consists of the following security areas (QUT, 2008):

Core Subjects

- Security
- Security Technologies

Optional Subjects

- Cryptology and Protocols
- Advanced Cryptology
- Computer Forensics
- Risk Management
- Cybercrime
- Privacy Law

Development of Security Curriculum

In the previous section, the paper illustrates that within an Australian context, security is taught via the following approaches:

Standalone Security Course

Niche Security Course

Embedded Security Course

What is of particular interest in relation to these courses is the following:

- all the security courses are heavily focused upon technology and therefore security is considered as mainly a technical issue;
- the majority of the security courses are specialised and are only taken by a small number of students. If the case of the *Embedded Security Course* example, the optional stream is one of 10 streams that can be taken by students (QUT, 2008).

Within Deakin University, Faculty of Business and Law, this shortcoming was recognised and the following issues addressed:

- security is a management issue and not only a technology issue;
- all Faculty students (whether undergraduate or postgraduate) should have the option to study Information Security as part of their course.

The decision was made to implement the *Embedded Security Course* approach at all levels and the outcome at the postgraduate level was (Deakin University, 2008a):

Enterprise Security Management Major

Law and the Internet

Electronic Crime

Risk Management for Business Information Systems

Business Security Management

Optional industry placement

This major is offered within the Masters of Business Administration and Masters of Commerce Course

The outcome at the undergraduate level was (Deakin Univeristy, 2008b):

Business Security Management Major

Information Systems Networks

Business Intelligence

Information Systems Management

Information Security and Risk Management

Plus optional units from:

Crime, Criminology and Policing

Law and the Internet

Small Business Systems

Information Systems and Global Issues

This major is offered via the Bachelor of Business Information Systems, Bachelor of Business Information Systems / Bachelor of Information Technology, Bachelor of Commerce and Bachelor of Management.

What is different in terms of this approach compared to other universities offerings is that:

- the security focus of the curriculum is from both a management and legal perspective;
- the majority of all students within the faculty can study Information Security as a discipline, which was a major aim of the draft 2002 Australian National E-Security strategy.

Development of Security Evaluation Framework

As described there is a lot of confusion about what Information Security is and what constitutes an Information Security course.

The authors have developed an initial Information Security Evaluation Framework (ISEF) which allows the courses of Universities to be evaluated. The framework determines the course type, which is:

Standalone Security Course;

Niche Security Course;

Embedded Security Course.

The framework then maps the index for the technical content and the business content of the course. All of this information is encapsulated within a network chart.

In the first example of the application of the ISEF, which can be found in Figure 1, is related to the evaluation of the undergraduate Information Security major offered at Deakin University.

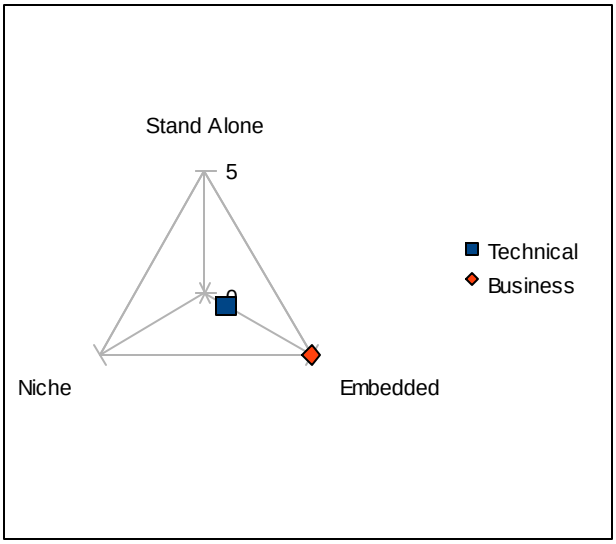

Figure 1: Deakin University – Undergraduate Information Security Major

In the second example, the authors evaluated the postgraduate Master of Information Systems Security at Charles Sturt University using ISEF, this can be found in Figure 2.

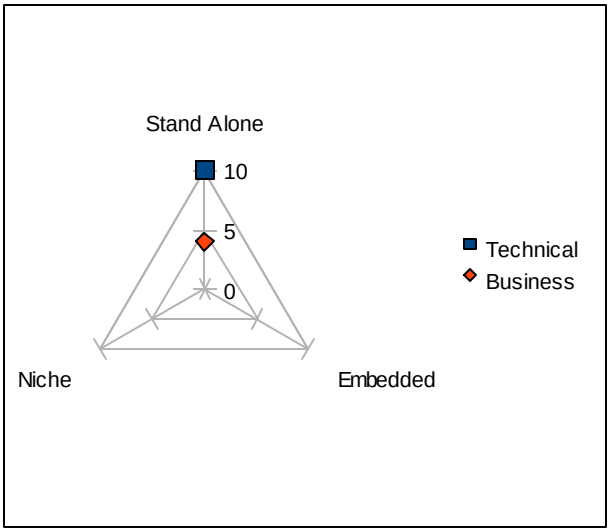

Figure 2: Charles Sturt University - Master of Information Systems Security

In terms of the ISEF analysis, it shows the different focus of courses. Figure 1 demonstrates the business focus of the undergraduate Information Security major and Figure 2 demonstrates the technical focus of the postgraduate Information Security Masters.

Conclusion

The major aims of the initial Australian National E-Security / Information Security strategy were to define key areas for Australia's development in terms of teaching and R&D but due to global events and political changes the Australian national agenda has changed.

In this fluid environment, Australian Universities have independently developed Security courses that they feel fulfil the requirements and meet the needs of industry. The authors intend to evaluate all Information Security across Australia using the ISEF method to give an understanding of

how different universities have developed their Information Security courses and the focus that these courses have taken.

References

ACM. (2008). *Computer science curriculum 2008: An interim revision of CS 2001*. Report from the Interim Review Task Force. Retrieved 10 December, 2008 from http://www.acm.org/education/curricula/ComputerScienceCurriculumUpdate2008.pdf

Aeuckens, D. (2001). *E-security skills, education and training in Australia: A policy scoping paper*. NOIE Report. Canberra, Australia.

Bogolea, B. & Wijekumar, K. (2004). Information security curriculum creation: A case study. *Proceedings of the 1st annual Conference on Information Security curriculum development*, Kennesaw, Georgia, USA.

Cant, S. (2002, June 24). Confusion reigns as NOIE role shifts. *The Age*. Melbourne, Australia.

Charles Sturt University. (2008). Course details - Master of Information Systems Security. Retrieved 10 December, 2008, from http://www.itmasters.com.au/security_multi.htm

Coonan, H. (2006). *Review of the e-security national agenda*. Media Release - Department of Communications, Information Technology and the Arts. Retrieved 10 October, 2006 from http://www.minister.dcita.gov.au/coonan/media/media_releases/review_of_the_E-Security_national_agenda

Deakin University. (2008a). Master of Business Administration - Enterprise Security Management Major. Retrieved 10 December, 2008 from http://www.deakin.edu.au/futurE-Students/courses/detail.php?customer_cd=C&service_item=M701&version_number=1&element_cd=SPECIALISATIONS-STR&sub_item_number=25&return_to=%2FfuturE-Students%2Fcourses%2Fcourse.php%3Fcourse%3DM701%26stutype%3Dlocal%26continue%3DContinue

Deakin University. (2008b). Master of Business Administration - Enterprise Security Management Major. Retrieved 10 December, 2008 from http://www.deakin.edu.au/futurE-Students/courses/detail.php?customer_cd=C&service_item=M305&version_number=3&element_cd=MAJORS-STRUCTURE&sub_item_number=3&return_to=%2FfuturE-Students%2Fcourses%2Fcourse.php%3Fcourse%3DM305%26stutype%3Dlocal%26continue%3DContinue

E-security review. (2008a). Attorney-General's Department. Retrieved 10 July, 2008, from http://www.ag.gov.au/esecurityreview

E-security review. (2008b). *E-security review: Terms of reference*. Attorney-General's Department. Retrieved 10 July, 2008, from http://www.ag.gov.au/esecurityreview

Edith Cowan University. (2008). Course details - Master of Digital Forensics. Retrieved 10 December, 2008 from http://www.scis.ecu.edu.au/Future/Courses/Postgraduate/922/Master+of+Digital+Forensics

Liles, S., & Kamali, R. (2006). An information assurance and security curriculum implementation. *Issues in Informing Science and Information Technology, 3*, 383-388. Retrieved from http://informingscience.org/proceedings/InSITE2006/IISITLile135.pdf

King, G. (2001). *Report on e-security R&D in Australia: An initial assessment*. NOIE Report. Canberra, Australia.

Howard, J. (2004). *Media Release – Fourth Howard Ministry*. Retrieved 10 May, 2006, from http://www.pm.gov.au/news/media_Releases/media_Release1134.html

Scott, B. (2001). *Media Release: Budget 2001-02 - Defence People Win*. MIN 144/2001, Department of Defence, May, Canberra, Australia.

QUT. (2008). Course Details - Masters of Information Technology. Retrieved 10 December, 2008, from http://www.courses.qut.edu.au/cgi-bin/WebObjects/Courses.woa/wa/selectMajorFromMain?structureID=22116&courseID=8190#22116

Tate, N., Lichtenstein, S. & Warren, M. (2007). Toward user evaluation of IT security certification schemes: A preliminary framework. *Proceedings of the IFIP TC-11 22nd International Information Security Conference*, Johannesburg, South Africa

Warren, M. J (2003). Australia: A national agenda for e-security education and research. In C. Irvine & H. Armstrong (Eds.), *Security education and critical infrastructures* (pp. 109-114). Kluwer Academic Publishers, USA.

Biographies

Professor. Matthew Warren is the Head of School and a Professor in the School of Information System, Deakin University, Australia. He has a PhD in Information Security Management from Plymouth University, UK. Professor Warren is the former Chair of IFIP TC 11 Working Group 11.1 - Security Management and a former Director of the Australian Institute of Computer Ethics. Professor Warren has taught within Australia, Finland, Hong Kong and the UK.

Dr. Shona Leitch is a Lecturer in the School of Information Systems, Deakin University. Shona is originally from Scotland, emigrating to Australia in 1998. She obtained her BSc(Hons) in 1997 from the University of Plymouth in Psychology/Computing. Her main teaching and research focus is the area of education and Information Systems. Dr Leitch has gained a PhD entitled "A Systems Analysis and Design Strategy for Online Teaching and Learning Systems" from Deakin University. Dr Leitch has also completed a Graduate Certificate of Higher Education. She has published over 25 papers, in books, journals and conferences, in the areas of systems analysis, online teaching and information security.