Proceedings of the 8th Colloquium for
Information Systems Security Education
West Point, NY June 2004

Embedding Industry Standards within the Undergraduate IT Security Curriculum: An Australian Implementation

Dr Jill Slay, *Member*, IEEE

Abstract—This paper responds to issues recently raised by Valli [1] and Schou [2] on the issues of the development of a modern undergraduate IT Security (Information Assurance) curriculum which links professional certification to academia. It details methods by which both industry standards, perspectives and research questions and also the (ISC)^2 body of knowledge may be embedded in the undergraduate IT Security curriculum and thus both academia and the IT Security profession may be satisfied.

Index Terms—IT Security Curriculum; Information Assurance; Industry Standards

I. Introduction

In recent work, researchers ([1],[2]) have highlighted a major issue in the development of modern IT Security (as Information Assurance is know in Australia) into the undergraduate curriculum. There is now a tendency for Australian universities to try to provide both an academic body of knowledge in IT Security as well as professional certification.

In his work Valli [1] contends that universities are at risk of failing to provide basic principles if they follow this path and states that they are falling into the trap of replacing sound foundations with technology specific data which will rapidly date:

> *"Universities should consider with gravity what it is that they are trying to achieve … This total curriculum replacement via industry certification substitution path is perilous and will see universities becoming vendor savants."*

Schou [2] notes the recent US initiative in allowing graduates from specified CAE schools to sit Certified Information Systems Security Professional (CISSP) or Systems Security Certified Practitioner (SSCP) exams. He question how this model can be used "as a basis for establishing standards for an international program for academia."

School of Computer and Information Science, University of South Australia, MAWSON LAKES, SA5095. AUSTRALIA
Phone: +61 8 83023840. jill.slay@unisa.edu.au
.

II. Principles Underpinning Undergraduate Coursework in IT Security at the University of South Australia

Currently I teach a 3rd year undergraduate course in It Security at the University of South Australia within the school of Computer And Information Science. This course is studied by approximately 350 students each year predominantly enrolled in the Bachelor of Computer and Information Science, Bachelor of Computing (E-Commerce), Bachelor of IT in Software Engineering, Computing and Multimedia and a range of other technical degrees. Students are located in 3 countries (Australia, Hong Kong Malaysia) and may also study totally externally or online. Principles which underpin our teaching are detailed here.

A. Holistic curriculum content

This course has been taught for about three years in its current format and needs about 25% update of content each year as the field changes. The prescribed text is familiar to most (*Security in Computing* by Pfleeger [5]). However, over the 2 last years, I have attempted to embed the Common Body of Knowledge used by the (ISC) ^{2} within it. So thus it has to contain:

1. Security Management Practices
2. Security Architecture and Models
3. Access Control Systems & Methodology
4. Application Development Security
5. Operations Security
6. Physical Security
7. Cryptography
8. Telecommunications, Network, & Internet Security
9. Business Continuity Planning
10. Law, Investigations, & Ethics

In Australia, all university programs in Computer Science (CS) also have to achieve the learning outcomes prescribed

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

by the Australian Computer Society (ACS) in order that the program may be accredited. Most CS or IT schools and departments also try to cover IEEE and ACM learning outcomes too.

Those who are familiar with Pfleeger's textbook will know that he does cover the basic Common Body of Knowledge used by the (ISC) 2 and probably the difference is the technical degree and the increased depth to which it is covered in a CS degree.

In summary, chapter titles in the 3rd edition include:

- Is there a security problem in computing ((ISC) 2 CBK 1)
- Elementary Cryptography ((ISC) 2 CBK 7)
- Program security ((ISC) 2 CBK 4)
- Protection in General Purpose OS ((ISC) 2 CBK 3)
- Designing Trusted OS ((ISC) 2 CBK 3)
- Database Security ((ISC) 2 CBK 4)
- Security in Networks ((ISC) 2 CBK 8)
- Administering security
- Legal, Privacy and Ethical Issues ((ISC) 2 CBK 10)
- Advanced Cryptography

(ISC) 2 CBK 3, 5 and 6 are somewhat diffused in Pfleeger but an experienced teacher can highlight these.

My conclusion is that there is in fact no high level conflict between (ISC) 2 CBK, ACM, IEE or ACS. I have mapped my own program curriculum to the CSSIP curriculum as shown and find that a student who has studied our undergraduate courses in object oriented programming and software engineering (and all do) plus my course in IT Security is then very well equipped to take and pass the CSSIP exam.

The teaching and learning problems which needs to be solved in the university, in this author's opinion, is firstly defining "graduateness" and secondly working out what is fundamental knowledge, what are foundational principles, for a graduate in CS who is going to work, or even carry out research, as maybe an entry level IT Security professional.

B. Defining graduateness

In seeking to provide a high quality learning environment that will prepare its students for life long learning, the University of South Australia [3], among others working in this field, has defined a series of generic learning outcomes that it desires to produce in its graduates. These can then act as measures of graduateness.
These include:

1. the ability to operate with and upon a body of knowledge of sufficient depth to begin professional practice
2. preparation for lifelong learning in pursuit of ongoing personal development and excellence in their professional practice
3. effective problem solvers, capable of applying logical, critical and creative thinking to a range of problems
4. commitment to ethical action and social responsibility as a professional and a citizen
5. the ability to work autonomously and collaboratively
6. effective communication skills
7. demonstration of an international perspective as a professional and as a citizen.

These infer that while the first graduate quality, the body of knowledge, is of primary importance, the method in which this knowledge is gained and applied is of equal importance and in fact to some degree defines graduateness.

This framework is then used as a basis for the design of teaching material both in a traditional and on-line mode and here we have used it as a framework to guide us in the production of holistic and cross-culturally student-friendly coursework.

All assessment pieces define which graduate qualities are being developed; if group skills are desired then group assignments which develop research skills in an IT security context are used. If individual report writing and information literacy skills are required then individual reports are requested

C. Gaining an Industry Perceptive

My local industry context is that the Australian defence industry and its major contractors are major employers of my graduates. The Information Warfare environment is one which is quite familiar to my students, particularly at a time of heightened awareness of terrorism, cyber-terrorism and computer crime. Readings from Denning [4] provide an excellent background too

I am fortunate that industry partners are able to supply research problems in wireless security and IW and so these issues supply a background to my undergraduate teaching and also the industry partners provide guest lectures. Student research work and particularly student theses are provided to my undergraduate students for extra reading.

The growth in computer crime and our local interest in forensic computing mean that our state police provide guest lectures in legal issues but also have provided resources for a module on forensic computing investigations.

Contextualizing the Australian university environment, it is important to realize that Australian universities, motivated by their need to compensate for the reduced amount of government funding and shifting demographics, and their prime location on the edge of education-hungry Asia, have moved quickly into the transnational learning market. This involves the teaching either

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

in traditional face-to-face or online mode of a range of programs, often with an IT focus, in countries such as Hong Kong, Malaysia, Singapore, India and China (PRC and ROC).

D. Mixed-mode and Resource Based Learning

Problems imposed by large classes in Australia over the last few years, and the large range of individual approaches needed to deal with some of student learning issues, computing academics have been some of the first to develop and use web-mediated networked learning environments for enhancing student learning, while maintaining a large proportion of traditional face-to-face tutorial and practical content within their subjects. The Web provides a vehicle for the development of the learning environment and teaching can be structured to develop lifelong learning skills and to cater for the expectations and learning styles of students from different cultures and backgrounds. We tend to call this mixed-mode delivery.

Mixed-mode delivery in our context implies that students are supplied with all learning resources online but teaching is augmented by lectures, practicals workshops and tutorials. This student-centered model shifts the focus off the lecturer as the supplier of knowledge, to that of the self-managed and autonomous learner being guided and supplied with resources to gain necessary knowledge in a graduate context..

We can argue that an IT Security professional is, of necessity a self –managed learner; our field changes so quickly that, although academics we are aware that foundations, theories and principles do not change, we know that the applications of theories and principles do. This mode of learning forces the students into what is usually an unwilling independence and increases the development of autonomy and self-motivation in learning

III. A CASE STUDY: SECURE AND HIGH INTEGRITY SYSTEMS

A. Holistic curriculum content

Applying my own principles as stated above in my introduction I explain the holistic nature if my teaching and the way in which I intend to teach the body of knowledge plus graduate qualities. I introduce my course thus:

> *"Computer and system security have become very complex issues in the Internet-enabled world of e-commerce, e-government and e-everything in which we live and work. In this course we start with an examination of the general issues in, and the terminology we come across when we examine, computer crime and information warfare (IW)*
>
> *We then look at protecting our distributed systems by the use of appropriate security controls and in the development of physical, technical and social IT and IS security policies, through the use of various risk management techniques. We subsequently examine the foundations of cryptography and cryptographic infrastructures that maybe use to hide information or for digital certification.*
>
> *We also take a general overview of operating systems and next look at the special meaning of "trust" in operating systems and compare Windows NT and Unix security. We then develop parallel overviews of networks and databases and determine how we can develop trusted networks and databases. We also take a brief look at hackers, the tools and techniques which they use to break into systems and the ways we, as security administrators, can harden our systems and protect ourselves.*
>
> *I have recently introduced a module which examines the special security issues involved in wireless networking and, for the first time, a module on computer forensics.*
>
> *This course is completed with a module which examines legal and ethical issues in greater depth and finally I will work through last year's exam to help you to understand my assessment requirements and to do well in the final exam.*
>
> *I am a strong believer in developing appropriate links between teaching and assessment and in this course I am focussing on helping you to develop information literacy, research and report writing skills while teaching you modern computer security. My assessment items are all contextualised as the kind of technical, well-referenced report you might have to write for your manager in your workplace. Information literacy, research and report writing skills will be developed in your workshops."*

Curriculum content follows Pfleeger and (ISC) [2]

- Trends And Issues In E-crime, Information Warfare (IW) and Computer Security
- Risk Analysis and Security Policies
- Database Security
- Trusted Operating Systems
- Basic Encryption
- Using Encryption
- Writing Secure Code
- Network Security Basics
- Threats To Network And System Security
- Wireless Security
- Computer Forensics
- Legal And Social Aspects Of IT Security

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

B. Defining graduateness and teaching the graduate qualities

I define the graduate qualities which I expect students to attain at the beginning of the course. I also teach these. This means that if students do not know how to reference or write reports then I have to teach referencing or report writing even in 3rd year of IT Security – I do get help in running remedial workshops.

I explain the development of the body of knowledge and graduate qualities in my course in this way:

Graduate quality	In relation to your course
Operates with and upon a body of knowledge	This course provides an overview of fundamental technical and organisational issues in IT security, sufficient for the commencement of professional practice
Preparation of lifelong learning toward personal development and professional practice	This course emphasises the development of Information Literacy through efficient search techniques, the development of literature reviews and summaries and presentation of results in written reports. These skills are important to industry and for research.
Effective problem solver applying logical, critical and creative thinking	Problem solving and critical thinking skills are developed through reading of case studies and the subsequent debate and analysis at workshops
Can work both autonomously and collaboratively	Students study both individually and in groups. Assignments will test individual skills – a final exam will test the students' individual comprehension of the course.
Committed to ethical action and social responsibility	This course examines IT security in a holistic manner, founded on the belief that ethical action and professional and social responsibility are basic to the development of true IT security.
Communicates effectively	This course develops one-to-one and one-to-many written communication skills
Demonstrates international perspectives	The IT industry is international and perspectives will be drawn from research and practice in Europe, Asia and USA.

Table 1 Graduate qualities achieved in Secure and High Integrity Systems

Students begin to know what is expected of then when they undertake the first assignment. In this case they are forced to consider both technical and societal issues and express them formally.

Report: Computer Crime, Information Warfare and Security – An International comparison

Graduate Qualities

By undertaking this assessment, you will progress in the development of the qualities of a University of South Australia graduate. The table below indicates the weighting—as a proportion of this assessment piece—given to developing one or more of the qualities

Table 2 Graduate Qualities achieved in Ass 1

1 body of knowledge	1.5
2 lifelong learning	1.5
3 effective problem solving	.1
4 work autonomously and collaboratively	.3
5 ethical action and social responsibility	.1
6 communicates effectively	.4
7 international perspectives	.6

Task

Write a 1000 word report (individual) drawing on the information presented in Module 1 and from other sources and discussing current trends in computer crime and information warfare and the kinds of measures that companies take to protect their IT infrastructure.

The Auscert 2003 Survey gives a good start but you will have to search relatively widely to find comparative trends in other countries. You MUST include data about two cultures other than your own. It might be helpful to look at European, American and Asian sources to get a balanced picture – you will find that there is a good survey available in Chinese from HKCERT.

It is made clear to students that they will be assessed according to the following criteria

- Professional Formatting of document
- Correct use of Harvard referencing
- Appropriate terminology and technical English – definition of computer crime and IW
- Quantitative (numerical and graphical) analysis of trends
- Qualitative (written in paragraphs, no dot points) analysis of trends
- Information from Culture 1

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

- Information from Culture 2
- Information from Culture 3
- Cross-cultural comparison

This kind of assignment forces students to think holistically. If they are presented with a marking scheme before they complete the assignment, they know that if they want high grade then, regardless of their country of residency and national culture, they will have to search for relevant information from at least other cultures and present it to me in a professional format. They are also aware that if they wish to pass well then they cannot use the "engineers' method" of providing a list of dot points and a chart. They must prepare their report in the same way that they might present the data to their employer in their first graduate IT security professional position.

C. Gaining an Industry Perceptive

An industry perspective is supplied in Australia by visiting lectures by SA Police, the Defence Science and Technology organisations and members of a small company supplying broadband via satellite to rural Australia.

Without prompting industry input always appears to be holistic and emphasizes:

- Importance of interaction of social and technical issues
- Need to understand legislation and act ethically
- Foundational need to carry out risk analysis and management and produce sound security policies
- Documentation and training

These are issues which are often neglected by CS academics and not thought of interest by their students but vital to practitioners.

In our teaching is SE Asia, we can provide a contextualized industry perspective by employing local tutors whose full-time employment is in the IT security industry. The current slump in Asian economies means that many IT professionals, often with masters' qualification in CS and business, are willing to support teaching. They bring anecdotes and examples of local practice to the classroom and can truly contrast academic theory with industry practice.

D. Mixed-mode and Resource Based Learning

In Hong Kong teaching involves 20 hours per course (over two separate weeks) of intensive face-to-face teaching by the Australian course coordinator and 10 hours of tutoring by a local tutor over the intermediate eight weeks. In Malaysia this involved 2 hour weekly tutorials given by a local tutor over twelve weeks. In these Asian cultures which are both incredibly diverse and also quite different to our Australian one, the learning issues are also different.

Major concerns which have arisen involve student's problems with the English language. While all students must pass University English language tests, Chinese students (and 99% of our HK and Malaysian students are of Chinese ethnic background with Cantonese or Mandarin as their first language) find it very difficult to read large amounts of text in English and to analyze and synthesize at the same kind of speed as a native speaker. Special attention has been paid to finding parallel Chinese language material (such as Government reports, papers and texts) to complement English resources. Students are not excused from reading and analyzing the English material but the Chinese is provided to augment their learning.

In our online environment we supply both a discussion board and the opportunity for synchronous chat with the lecturer for students who cannot get to the campus. While students in their earlier years in Hong Kong made good use of the chat session we now find that they prefer to use the discussion board, supporting each other with resources and also offering support and encouragement or even the odd rebuke from one classmate to another who displays an overly negative attitude.

IV. Discussion and Conclusion

My hypothesis is, in response to Valli [1] and Schou [2], that it is possible to map the (ISC)^2 CBK to undergraduate curriculum and to teach industry standards with proper academic rigour. How we evaluate the effectiveness of what, in my case has to be seen as a pilot, I am not yet sure.

A. Student grades

Results in Australia after two deliveries to approximately 400 students in total show an overall failure rate of 6% (largely due to poor English) with an average grade of a high credit (approximately 70% credit)

Results in Malaysia to a group of approximately 40 showed a very similar average mark with a much higher failure rate (50%) which is also due to poor language skills. Teaching in HK is still ongoing but indications are that pass rate and average mark will be similar to Australia.

Longer term tracking and evaluation and a thorough statistical analysis are needed to draw any trends from this data.

B. Conclusion

Our experience over two years indicates that mixed-mode teaching is a reasonable alternative to face-to-face teaching transnationally and can be used to enhance student's

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

development of information literacy and lifelong learning skills and support a holistic understanding of IT security which does link industry standards to undergraduate curriculum

Other issues which need to be faced though as we spread further and further geographically with our teaching, is the irony of teaching IT Security within an Information Warfare context to such a broad range of cultural groups. As we begin to instill in students from a wide range of backgrounds some of the foundations of defensive cyber warfare we have to ask what it means to teach potential "adversaries" (and maybe not even our own adversaries) the basics of such a war. This forces us to draw back and ask again "what is holistic IT security and how should it be taught"?

We are also challenged by the nature of industry input in the countries where we teach. While sophisticated SE Asian nations have highly qualified and international corporate player working in this arena, our newer partners are located in less well-developed economies. In some locations there may be more opportunity to support a country in setting national IT security standards than in embedding their national ones within our localized Australian curriculum

V. REFERENCES

[1] Valli, C. (2003) *Industry Certifications: Challenges For The Conduct Of University Security Based Courses, I*n 4th Australian Information Warfare and Security Conference(Ed, Slay, J.) University of South Australia, Adelaide.

[2] Schou, C. (2003) *Standards, Standards, Standards -- Who has the Standards? I*n 4th Australian Information Warfare and Security Conference(Ed, Slay, J.) University of South Australia, Adelaide.

[3] University of South Australia. 1996. *Guide to implementing the qualities of a University of South Australia graduate in course and subject development.* Unpublished internal paper.

[4] Dorothy Denning, *Information Warfare and Security,* Addison Wesley, 1999.

[5] Pfleeger, Charles, P. (1997) Security in Computing. 3rd Edition. Prentice Hall. ISBN 0-13-035548-8

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE