Journal of Information Systems Education, Vol 13(3)

Securing the Commercial Internet: Lessons Learned in Developing a Postgraduate course in Information Security Management

Sophie Cockcroft
UQ Business School
University of Queensland
Brisbane, QLD 4072, Australia
s.cockcroft@business.uq.edu.au

ABSTRACT

This paper describes the inception, planning and first delivery of a security course as part of a postgraduate e-commerce program. The course is reviewed in terms of existing literature on security courses, the common body of knowledge established for security professionals and the job market into which students will graduate. The course described in this paper is a core subject for the e-commerce program. This program was established in 1999 and the first batch of students graduated in 2001. The program is offered at both postgraduate and undergraduate level. The work described here relates to the postgraduate offering. Students on this program are graduates of diverse disciplines and do not have a common e-commerce or business background.

Keywords: Information security management, postgraduate education, is curriculum, is job categories.

1. INTRODUCTION

The importance of security in the IS and particularly the e-commerce curriculum cannot be over-emphasized. Trends towards globalization including virtual teams and mobile/wireless computing force this area to be addressed more thoroughly.

Establishing and running an information security management course in a business school presents a series of unique challenges. It is important to assume a management focus without underemphasizing the importance of technical competence. Thus theoretical and practical aspects have to be balanced. This paper describes the first run of a security course designed specifically for managers within a postgraduate e-commerce master's course.

This paper is divided into four parts: First the inception of the course and demographics of the first intake are described. Next, the curriculum design of the current course and the course content is described. Finally the course is evaluated: first by traditional means, i.e. student evaluations and comments and by contrast to literature on other security courses; and second by way of a study of the Australian job market for security to ascertain whether the course is meeting its proposed market, and it is set in the context of an established common body of knowledge**.**

1.1 Background

The first enrollment of students in the course described here, entitled "Securing the commercial internet," was in March 2001. One-hundred students enrolled, 88 of which were pursuing a master of commerce, specializing in e-commerce. The remainder was made up of: five masters level financial management students, five masters level information technology students, one MBA student and one using the course to complete a degree from another institution. Many of the students were studying part time whilst undertaking paid work outside university.

Securing the commercial internet was established as a required, standalone course within an e-commerce program. At the inception of the course the stated aim of the e-commerce program was to graduate "students who understand business and are familiar with the latest eCommerce technologies" and to provide "industry with suitably qualified e-commerce staff" (UQ Business School 2001). The economic justification was to meet the burgeoning demand (Towers Perrin 2000) of the e-commerce industry locally and globally. Whilst demand for e-commerce staff *per se* has waned somewhat,

security is still touted as a top role or skill required by IS professionals (CareerOne 2002) in Australia. It is likely that demand for information security managers has risen in the wake of events of September 11th.

The initial offering was developed in cognizance of:

- the strengths of the school,
- literature and textbooks,
- fit with the Australian context.

The school has demonstrated teaching and research strengths in the area of Information Systems Control and Audit. At the inception of the course these aspects were emphasized in the course catalogue. Its description was as follows:

"[This course] covers controls and audit procedures associated with preserving authenticity, accuracy, completeness, timeliness, and privacy of electronic transactions over the Internet and quality assurance for electronic commerce applications."

A number of textbooks were reviewed. The textbook finally selected for the course (Greenstein and Feinman 2000) also reflected the schools interest in IS Audit and accounting perspectives on security. The textbook is well supplied with cases and tutorial material, covers the technical aspects of ecommerce, and gives explanations that would be easily understood by accountants (Heales 2000). This was supplemented by a handout (reader) containing 19 academic papers complementing the text book, in particular emphasizing the Australian context that is missing from the textbook, which has a North American focus. For example, some of the papers in the reader concerned standards in the Australian context as promulgated by the National Office of the Information Economy (NOIE) (NOIE 2002) and standards Australia (Standards Australia 2002). The Australian approach to privacy law differs markedly from the North American approach; papers reflecting this difference were also included in supplementary reading.

The following course description and objectives evolved:

> "Individuals who complete this course will have a level of insight into Internet security appropriate to managers in businesses using electronic transactions. In particular they will be able to identify the strategic value of security to a firm and formulate plans appropriate to the business concerned. They will be able to independently assess the adequacy of existing security mechanisms within an organization from the technical and managerial perspective. In addition they will understand how the legal concepts of privacy and trust in electronic commerce relate to issues of security. They will be able to analyze the efficacy of data protection within electronic commerce systems particularly with respect to internal controls. They will be able to describe testing techniques and audit procedures, which may be used to detect deficiencies."

1.2 Course Objectives

Research Aspects

- Gain insight into current issues in commercial internet security
- Identify and assess risks to security within an e-business and formulate security conscious solutions,

Technical/System Development aspects

- Describe the main technologies for implementing security. Specifically;
- Security standards and protocols
- Encryption
- Authentication
- Firewalls

Third Party Assurance

- Apply audit and control principles to the e-commerce environment and electronic financial systems with respect to:
- Asset safeguarding
- Data Integrity

Regulatory Environment

- Demonstrate an awareness of consumer privacy rights and their impact on commercial internet security

The objectives are themed according to the roles of different professional groups in security (i.e. accountant, lawyer, IS professional). The importance of identifying themes within a course was highlighted by Deans (1993). This is because, as the course evolves, major topics can be related back to these themes. In addition, these themes are implicit in the course text Greenstein and Feinman (Greenstein and Feinman 2000). Finally the professional issues theme was chosen because of the diverse backgrounds of the students entering the course. The theme allows students to actively contribute to class discussions in their areas of knowledge. The course was delivered in flexible mode with materials and quizzes being available through WebCT, although attendance at tutorials was required.

2. CURRICULUM DEVELOPMENT

The approach to including security in the IS curriculum varies from school to school; the main options are inclusion of a single course devoted to security, or spreading the teaching of ISM across areas where it has relevance. Schools have to decide whether such a course should be mandatory or optional. Further to this, teachers have to establish what areas from the common body of knowledge should be included in the course. Both positioning of security within the curriculum and whether it should be optional or not were explored in Anderson and Schwager (Anderson and Schwager 2002). At the school where this course is run, we were lucky to be developing an entire program from scratch. Thus there was some freedom in designing the program so that whilst security is offered as a standalone course it always runs concurrently with other relevant courses such as infrastructure management. Faculty on both courses work closely together so that students pick up

required network management knowledge along with an awareness of security issues.

3. COURSE CONTENT

The main learning goals and activities in the course are summarized in Table 1.

Table 1: Course Content

Learning Goal	Activities	Assessment
Insight into current issues in Commercial Internet Security	**Group presentation Structured Peer Feedback Video Showings Involvement in Virtual Economy**	**Group Project (Presentation plus research paper) Peer review**
Identify risks to organizations and formulate solutions	**Price Waterhouse Guest lecturer and class discussion. AUSCERT guest lecture. Security Audit**	**Security Audit**
Describe technologies that support secure e-commerce ▪ Security standards and protocols ▪ Encryption ▪ Authentication ▪ Firewalls	**Various hands on lab work**	**Exam**
Third Party Assurance	**Practical work installing Digital IDs for E-mail and Digital Certificate for server.**	**Case Study 1 (Comparison of key issuing companies)**
Regulatory environment	**Privacy Survey (examining own attitudes to privacy)**	**Case study 2 (Privacy comparison between two countries)**

Each learning goal is coupled with activities to support it and at least one assessment item to reinforce learning. The research aspect of the course is designed to help students get up to speed with current issues in the security arena. In groups, a paper was selected from the handout (reader) to form the basis for wider research and a presentation. Individually, students provided feedback to the groups in a peer review. A mark was awarded for the quality of the review, each student had to produce four of these reviews and hence attend at least four presentations. The topics of these presentations and research papers are given in Table 2.

3.1 Research Activities

The students of this course visited the virtual economy, run by students of the School of Library and Information Science at Indiana University, (Rosenbaum 2000). As shoppers they were able to pick up relevant security references to help with their assignments and presentations. The relevance of material "on sale" was assured since students of the Indiana course had contacted the course coordinator of the present course prior to the start of semester to identify areas in which they should provide information.

Table 2: Presentation Topics

Penetration testing/Auditing
Information warfare
Risks of Mobile E-commerce/Wireless application security
Risk Management/Disaster Recovery
Firewalls
Electronic Money/SET/SSL
Security Standards

3.2 Security Audit

A common feature of IS security courses is the security audit of a real firm. Many educators take the view that aspects of security management cannot be learned in a classroom alone (Smalling and Sloan 2000). There is much to be gained by tackling a real-life audit. In particular, hands on experience with security risks to which organizations expose themselves and interaction with other technical and security managers is of great value. The security audit was offered in the first year that the course ran. Students were required to find companies willing to undergo a security audit and put them in touch with the course coordinator. In all cases, a letter was issued to participating companies stating the boundaries of the audit. In particular, it stated that they would not be charged, that the students undertook to adhere to the privacy policies of the organization, that the work did not require direct access to electronic resources or sensitive data, and that penetration testing would not be used to assess vulnerability. In some cases the firms wrote back requesting variations, which were incorporated in a modified letter. In the case of one government department this took the form of a request that all copies of the report, electronic and otherwise, should be returned to them after marking. The audit proved hard to administer. Students failed to find companies that were prepared to submit themselves to a rigorous audit. Those who find willing participants were most likely to be working in the organization themselves. Whilst the audit ran without incident, it remains a concern, in a similar

way to that expressed by one of the respondents in the Anderson study (Anderson and Schwager 2002), that there could be legal action against the school if any computer related criminal activity subsequently emerged within the organizations audited.

3.3 Lab work

Various technical lab-based exercises complement the theoretical content of the course. This is considered important because graduates of this course need a degree of practical competence to effectively interface between managers and system developers in the security arena.

Testing: Students first undertook a review of a sample web based system from the point of view of security, in particular with respect to logins, directory structure, directory browsing and the risks of active content. This could be seen as a very cut down version of a penetration test.

Firewalls: Students undertook an exploratory study using the free trial version of Zonealarm (Zonelabs 2002). This involved customising the firewall to meet business rules based on IP address or software accessing the firewall. Students locked out selected IP addresses and used the "ping" function to discover which other students were locking them out by means of a firewall. The packet sniffer Ethereal was used to investigate what packets were travelling either side of the firewall. All this was carried out in a secure lab, isolated from the rest of the public university machines.

PKI and third party assurance: Students installed a digital ID from Thwarte or Versign in conjunction with their e-mail browser and sent signed and/or encrypted e-mails. In addition they went through the process of installing a digital certificate on a web server to learn how a secure server works.

Encryption: Students used a piece of demo software "encryptor", developed in the school, which illustrated the different forms of encryption, by encoding and decoding sentences.

Cookies: Students ran a web server from their lab machine and wrote software that implemented a cookie on a web site they developed, and then visited other student's web sites. A discussion relating to the use and abuse of cookies was conducted.

3.4 Privacy

Students were encouraged to raise their awareness of their own attitudes toward information privacy by participating in a survey. The questions were drawn from a validated instrument by Milberg et al (1995). The results were then presented back to the class and compared with those of other studies (Alexander 1998) (Vance 2000).

3.5 Guest Lectures

Guest lecturers were invited to talk to the class in the risk management area. These came first from the Australian Computer Emergency Response Team (AUSCERT) and second from the technology risk management division of Price Waterhouse Coopers.

4. EVALUATION

4.1 Student Feedback

The course was reviewed by the usual means of student evaluations. Interestingly, questions relating to the value of the course yielded higher scores than those relating to the instructor. This could have to do with the large amount of material, quizzes, hyperlinks and learning guide available on line.

Comments from the students indicated that the textbook had too great a focus on accounting issues, and that there was some overlap with courses they were taking, for example, in the law school – this needs to be reviewed. There were also positive comments regarding the lab work, including requests for more emphasis on this part of the course. The difficulty with this is that a similar course with a definite technical focus is currently running in the faculty of information technology and electrical engineering. The solution here may more likely lie in improving the managerial parts of this course. This could involve expanding on the security audit, or incorporating a real-life continuity planning exercise as described in (Smalling and Sloan 2000). From the risk management part of the course students gave positive feedback on guest lecturers.

4.2 Post Script

Two aspects that were not taken into account in the first delivery of the course were: how well this course fits with the common body of knowledge for security professionals (ISC2 2000) and how well it meets the local employment market. As part of the evaluation of the course and as an indicator of where further work might be necessary, the following section provides a brief overview of these aspects.

Common Body of Knowledge: Table 3 illustrates the main topics from the common body of knowledge (CBK) (ISC2 2000) illustrating which parts are addressed by the current course.

The market for information security managers: Thirty three job advertisements were selected from online job sites (JobNet 2002) (Byron 2002). Jobs were selected according to the following criteria. They were placed during the three months March-May 2002, from within Australia, and containing the key word security in either the title or the body of the advertisement. They were searched using the topic list put forward by ISC2 (ISC2 2000). The results illustrated in Table 4 show the top 12 most frequently occurring skill requirements in this selection.

Table 5 gives a breakdown of the job titles. Repeating titles have been omitted.

Table-3: Common Body of Knowledge

CBK TOPIC	Central to course	Comment
Access control systems and methodology	✓	**Only methods of attack, monitoring and penetration testing emphasized**
Telecommunications and Network Security	✘	**Largely covered in companion infrastructure course (except firewalls)**
Security Management Practices	✓	**Of central importance**
Applications and System Development security	✓	**Data mining only mentioned. Mostly reserved for practical work**
Cryptography	✓	**Covered with respect to its support for confidentiality, Integrity, Non-repudiation and authenticity**
Security Architecture and models	✘	**Out of scope of course**
Operations Security	✓	**Only in terms of monitoring and intrusion detection. Much of this material covered in IS audit course in school.**
Business continuity planning & disaster recovery	✓	**Of central importance**
Law, investigations and ethics	(	Only in terms of privacy and trans-border flow
Physical security	(	Out of scope, only passing coverage

5. RESULTS

Reviewing the course in terms of its fit with the common body of knowledge for certified information systems security professionals (ISC2 2000) the course does not go into great detail on network security, security architecture and physical security. It is suggested that the first two of these topics find their place more properly in the sphere of computer science.

Turning to the demands of the local job market, whilst it is hard to generalize from such a small review, it is likely that the emphasis on privacy reflects the recent changes in privacy laws that came into effect in Australia in December 2001 (Privacy Commissioner 2001). Private sector organizations have rushed to ensure that their policies are in line with the new amendments. In this respect the students are well equipped to meet the job market in the privacy area.

This brief review also supports the view put forward by respondents in the Anderson and Schwager study

Table 4: Skill Set For Information Security Managers

Key word	Occurrences
Risk	18
Privacy	12
Policy	9
Communication skills	7
E-commerce	7
Technology standards	5
Company standards	5
Firewalls	5
Security strategy	4
Government standards	3
Access control	**3**
Public key infrastructure (PKI)	**2**

Table 5: Typical Job Titles

Data Warehousing/ Information Manager - Data strategy and Information e-commerce, government experience
Head of Information Security
Information Security Advisor - security strategy, data management, Information Security Manager
National Sales Manager - Security
IS Security Manager
Risk/Security Manager
Sales Manager - Security
Security Manager
Technical IT Security Manager
Analyst Programmer
Analyst/Programmer – Security
e-commerce Security Consultant
Information Security Advisor - security strategy, data management, e-commerce, government experience Information Security Manager
IS Security Engineer/Administrator
Privacy Project Manager

(Anderson and Schwager, 2002) that security courses should focus on managerial strategies and policies rather than technical details. Risk management is well represented in the job advertisements. More activities in this area might strengthen the marketability of the course. Getting the students to present the results of their research is a small step in improving communication skills, which appeared frequently as a valued attribute. Technology standards and technical details such as setting up firewalls and Public Key Infrastructure (PKI) still appear in these advertisements. This in some way justifies the inclusion of these topics in the course outline.

6. CONCLUSION

This paper has explored the issues raised in developing a course for commerce students in information security management. One benefit of the structure of the program is that it runs in conjunction with an infrastructure management subject, which is also a core subject, so the majority of the students are developing complementary technical knowledge along the way. Assignments involving security audit require careful monitoring and dissemination of information to all parties involved. The aim, in reporting the setting up and running of this course, is to provide comparison and the benefit of hindsight to those thinking of undertaking similar endeavours.

7. REFERENCES

Alexander, P. [1998]. Attitudes Toward Information Privacy: Differences Among and Between Faculty and Students. The AIS Americas Conference, Baltimore, Maryland, August 14-16, 1998.

Anderson, J. and P. Schwager [2002]. "Security in the Information Systems Curriculum: Identification and status of relevant issues." Journal of Computer Information Systems Spring.

Byron [2002]. Byron Employment Australia, http://employment.byron.com.au, 22/4/02

CareerOne [2002]. Roles and skills that are hot right now, http://careerone.com.au/common/news_story/0,6206,resources|resgetjob^4447681,00.html#it, 22/7/02

Deans, C. [1993]. "International information systems and Technology: course development and Implementation." Journal of Information Systems Education 5(2).

Greenstein and Feinman [2000]. Electronic Commerce: Security, Risk Management and Control. New York, McGraw Hill.

Heales [2000]. "Book Review: Electronic Commerce: Security, Risk Management and Control." Accounting and Finance 2(2000): 188-190.

ISC2 [2000]. Certified information systems security professional common body of knowledge study guide, www.isc2.org, ISC2, 12/4/2002

JobNet [2002]. JobNet: The career centre for IT&T professionals, http://www.jobnet.com.au, JobNet, 28/4/02

Milberg, S., S. Burke, et al. [1995]. "Values, personal information, privacy and regulatory approaches." Communications of the ACM 38(12): 65-74.

NOIE [2002]. National Office of the Information Economy, http://www.noie.gov.au/, NOIE, May 2002

Privacy Commissioner [2001]. About Privacy in Australia, http://www.privacy.gov.au/act/index.html#2.1, Privacy Commissioner, 3/4/2002

Rosenbaum, H. [2000]. Ecommerce education using a virtual economy, http://www.indiana.edu/~rindiana/2000/poster/rosenbaum_e-commerce/slide01.html, 12/4/02

Smalling, G. and S. Sloan [2000]. "Not by books alone." Security Management 2000(October): 51-54.

Standards Australia [2002]. Standards Australia, http://www.standards.com.au, June 2002

Towers Perrin [2000]. "E-literacy shortage." Australian Financial Review,, 1: 19.

UQ Business School [2001]. Undergraduate Handbook. Brisbane, University of Queensland**:** 1-15.

Vance, D. A. [2000]. On the effects of exogenous and endogenous variables on information privacy concerns: a preliminary comparative study. Challenges of Information Technology Management in the 21st Century. 2000 Information Resources Management Association International Conference., Hershey, Idea Group Publishing.

Zonelabs [2002]. Zonelabs, www.zonelabs.com, March 2002

AUTHOR BIOGRAPHY

Sophie Cockcroft is a Lecturer in Information Systems and E-commerce at the UQ Business School. Before joining UQ she taught at the University of Otago in New Zealand and City University in Hong Kong. Her research interests include system development, data quality, security and privacy. She holds a Ph D in Information Systems from the University of Otago.

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