Teaching Information Security Management: Reflections and Experiences

Atif Ahmad
Department of Computing and Information Systems,
Melbourne School of Engineering,
The University of Melbourne, Australia.

Sean B Maynard
Department of Computing and Information Systems,
Melbourne School of Engineering,
The University of Melbourne, Australia.

Corresponding author: Atif Ahmad
atif@unimelb.edu.au

Abstract

Purpose: This paper describes the development, design, delivery and evaluation of a post-graduate information security subject that focuses on a managerial, rather than the more frequently reported technical perspective. The authors aimed to create an atmosphere of intellectual excitement and discovery so that students felt empowered by new ideas, tools and techniques and realized the potential value of what they were learning in industry.

Approach: The paper develops fundamental principles and arguments that inform the design and development of the teaching curriculum. The curriculum is aimed at security management professionals in general and consultants in particular. The paper explains the teaching method in detail including the specific topics of lectures, representative reading material, assessment tasks and feedback mechanisms. Finally, lessons learned by the authors and their conclusions are presented as a form of reflection.

Findings: The instructors recognized four key factors that played a role in the atmosphere of intellectual excitement and motivation. These were new concepts and ideas, an increased level of engagement, opportunities for students to make their own discoveries, and knowledge presented in a practical context. Maintaining a high quality of teaching resources, catering for diverse student needs and incorporating learning cycles of assessment in a short period of time were additional challenges.

Originality / value: Most ‘information security’ curricula described in research literature take a technology-oriented perspective. This paper presents a much-needed management point of view. The teaching curriculum (including assessment tasks) and experiences will be useful to existing and future teaching and research academics in ‘information security management’. Those interested in developing their own teaching material will benefit from the discussion on potential topic areas, choice of assessment tasks and selection of recommended reading material.

Keywords

Information Security Management; Information Security Manager; Education; Teaching; Curriculum Development;
1. Introduction

Managing information security in organizations requires the application of a range of formal, informal and technical security controls to address complex security risks. In addition to excellent management skills, information security managers need a keen understanding of how security supports business objectives, as well as a broad working knowledge of a number of security practices.

Unfortunately, ‘information security’ education in most universities takes a largely technology-oriented perspective (Mullins et al. 2007; Malladi et al. 2007; Dark et al. 2006; Hentea et al. 2006). An informal survey of curricula across the university sector, including professional training, reveals instruction revolves around the understanding of technology vulnerabilities, network security protocols, configuration of countermeasures, application of cryptography and the like (Sharma & Sefchek 2007). Of the few subjects that adopt a broader view of security, the non-IT content frequently focuses on privacy, ethics, and legal considerations rather than on strategic management skills (Bishop & Frincke 2007; Sharma & Sefchek 2007). Given that a major focus of information security in organizations is at the strategic management level, this lack of a broader security perspective fails to adequately train students in information security management.

This paper presents the authors’ approach and experiences in the development, design, delivery and evaluation of a post-graduate level elective subject titled “Information Security Consulting” at the University of Melbourne, Australia.

The primary teaching aim of the authors is to impart the fundamental principles of information security management. This subject familiarizes students with the practices and processes involved in managing information security at an enterprise-wide level: conducting an information security risk assessment, evaluating the quality of a policy, recognizing the range of security strategies available and how they relate to controls, and devising an effective security education, training and awareness program. Additionally, the subject exposes students to a range of technical security controls, their strengths and weaknesses and appropriate usage.

This paper is structured as follows. First, research in the area of IT and Information security is discussed. The paper then describes the development, design, delivery and evaluation of the information security consulting subject. The paper then discusses the lessons learned and some reflections on the subject as a whole.

2. Content Matters: From IT Security to Information Security

A number of universities have introduced new teaching initiatives in the general area of information security (Mullins et al. 2007; Malladi et al. 2007; Dark et al. 2006; Hentea et al. 2006). In their review of information security education in the USA, Sharma and Sefchek (2007) point to the large number of security subjects offered in the IT faculties of Universities since 1997. Security education has added significance due to sponsorship by the US federal government such as ongoing initiatives by the National Security Agency (NSA).

A comparison of curricula in the USA and China reveals that whilst security programs mainly cover the technical aspects of IT security, there is some emphasis, especially in the USA, on Information Security, but not necessarily on its management (Chen et al. 2013). Subjects tend to have titles incorporating terms such as “Computer Security”, “Computer and Network Security”, “IT Security”, “Information Security” and “Information Assurance”. A closer look at the curricula reveals a focus on threats, vulnerabilities and countermeasures as they relate to information technology. These subjects aim to teach students to secure information technology using a comprehensive and systematic approach using theoretical and/or practical methods. This implies that security subjects, especially in China, adopt a strongly technical or engineering perspective as opposed to a management perspective.

Although these “technical” subjects are both necessary and critical to the development of future generations of IT security professionals, they are not particularly suited to management personnel for three main

---

1 In this paper we use the Australian definition of the term “subject” which is equivalent to the term “course” in USA terminology. It represents a coherent unit of study that makes up a larger area of study.
reasons. Firstly, IT security subjects focus on examining technical controls rather than formal controls such as Security Risk Management and Security Policy, and informal controls such as Security Education, Training and Awareness (SETA) (see Dhillon 2007 for the rationale behind classifying controls into formal, informal and technical categories). Security management professionals require a background in strategic aspects of enterprise security such as Risk Management, Culture, Governance, Policy, and SETA. In particular, it is important that discussion of formal and informal controls occurs in the context of organizational issues such as the impact on business processes and cost, as well as the perspectives and needs of various stakeholders including senior management, middle management and end-users as well as stakeholders outside the organization such as vendors, clients and regulatory authorities.

Secondly, focusing exclusively on IT security tends to result in a narrow view of ‘information’, centering on the digital environment whilst ignoring the physical environment where information is stored in hardcopy form and the cognitive environment such as in the minds of personnel (Ahmad et al. 2005). Key topics, such as secure knowledge management and secure handling of hardcopy documentation, are not typically covered in these IT security subjects. A broader enterprise view of information security should embrace the need to protect information and knowledge of different levels of sensitivity even if these reside outside the digital environment. To acquire this area of expertise students need a background in more traditional information systems and management disciplines. In particular, an understanding of knowledge management is critical, especially the difference between tacit and explicit knowledge as well as how knowledge is acquired, combined and shared amongst human networks.

Thirdly, IT security addresses the security problem from a technology centric perspective rather than a people centric perspective. Given over half of all Information Systems Security breaches are caused by employees failing to comply with procedures, it is particularly important for an Information Security Management subject to address the human dimensions of Information Security (Vance et al. 2012).

From the above discussion, teaching Information Security Management (ISM) should reflect the following principles:

- Principle 1: Information security aims to protect the business function of the organization and therefore must be aligned to strategic business management
- Principle 2: Information security aims to protect information and knowledge wherever it may be stored and however it may be transmitted
- Principle 3: Information security is essentially a people problem that has some technical solutions.

3. Subject Design and Delivery

“Information Security Consulting” is a postgraduate level elective subject offered by the Department of Computing & Information Systems at the University of Melbourne. Choosing a suitable name for this subject was particularly challenging as there is considerable confusion surrounding the precise boundaries of the discipline of ‘information security’. This is exacerbated by the number of terms used interchangeably to describe the “information security” field. For example, ‘computer security’, ‘information technology security’, and ‘information assurance’ are considered by many in the public domain to be approximately the same as ‘information security’. According to Myers & Riela (2008) the field of security used ‘computer security’ and ‘network security’ to describe itself early on when the focus was on protecting individual computing items. When the focus moved to protecting larger systems then these words were replaced by ‘information security’ and the like.

The authors considered each of the above terms in their choice of a subject name. For an Australian audience there are few advantages in using ‘information assurance’ in the title of the subject as the term is not commonly used in Australia. The terms ‘IT Security’ and ‘computer security’ are misleading as the instructors are teaching a management oriented subject rather than a technical one. The term ‘information security’ is frequently used in Australian Universities to house content in the area of cryptography, which is also not the intention of the instructors. However, by adding the term ‘consulting’ to “information security” serves two purposes. Firstly, it lends a distinct management flavor to the title which orients prospective students and employers to the intended content area. Secondly, it attracts students pursuing a career in management consulting. This makes practical sense since a large percentage of information systems
graduates at the University of Melbourne are recruited by top tier management consulting firms such as Deloitte, PriceWaterhouseCoopers, KPMG and Accenture.

This section describes the development, design and delivery of the information security consulting subject. The subject was designed with the three principles in mind from the outset. This section first details the teaching approach used. Subsequently it describes the content of the subject, the student audience and the assessment practices undertaken.

3.1. Teaching Approach

In designing and delivering this subject, the authors were motivated by two key teaching objectives. Firstly, the subject content must be designed to target the needs of the modern information security management professional and consultant. As such, each of the principles discussed in section 2 must be incorporated into the subject design. Therefore, the subject content must focus on formal and informal controls and have a focus that shows that information security is a people problem that has technical solutions (Principle 3). Attention must also be paid to understanding the range of technical security threats and the implications for organizations. Since information security managers must have a working knowledge of technical security controls, therefore attention must be paid to their tactical deployment. As mentioned in Principle 2, the content must also cover secure knowledge management and the security of information outside the digital environment. Also the subject needs to incorporate that security must be aligned to the strategic management goals of the organization (Principle 1).

With the first teaching objective in mind, the instructors looked at a range of security textbooks. Unfortunately the vast majority take a technical perspective (for instance: Practical UNIX and Internet Security - Garfinkel et al. (2003), Security in Computing – Pfeeger & Pfeeger (2006), Introduction to Computer Security – Bishop (2004); Computer Security – Golman (2009)). Of the few information security management textbooks available the authors selected ‘Principles of Information Security’ (Whitman and Mattord 2012) as it was appropriate introduction to information security for non-technical students and provided comprehensive treatment of formal and informal controls such as security risk management, security policy, SETA, and security planning and strategy (Principle 1). In particular, the chapters on technical security threats, attacks and controls were suitable for students without a technical background. Further, the textbook discussed information security from a business/people point-of-view except where the topic was security technologies or network and system attacks (Principle 3). However, the instructors did not feel the textbook adequately covered secure knowledge management and information classification especially in the context of physical and cognitive environments (Principle 2). Other sources needed to be found to cover the consulting content and other advanced topics like that of intelligence collection. The instructor felt that his own experience was sufficient to cover the material on consulting practice. For the intelligence content, Lowenthal’s ‘Secrets to Policy’ text was chosen (Lowenthal 2006).

Secondly, the instructors wanted to create an atmosphere of intellectual excitement and discovery so that students felt empowered by new ideas, tools and techniques and realized the potential value of what they were learning in industry. Previous research has shown that ‘intellectual excitement’ is a powerful motivator for student learning (Wlodkowski 1999). It stimulates curiosity and a genuine desire to learn which ultimately results in improved learning, engagement and development among students and instructors (Pascarella & Terenzini 1998). The authors decided to stimulate discussion by dividing the student cohort into groups. Each group was assigned a security theme to champion in every discussion and debate throughout the subject. The student cohort was divided into five groups of 6 to 7 students. The themes were ‘Security Strategy’, ‘Security Culture’, ‘Security Risk’, ‘Security Policy’ and ‘Security Technologies’. Each group was provided a list of seminal research papers from where knowledge can be drawn (see Table 1) and was encouraged to also read additional papers outside of the list.

Another method used to stimulate discussion was to present ideas and principles in a broader and practical context. The instructor drew on his previous experience as an information security consultant for examples and scenarios. For example, the lecture on security policy was presented with examples from real and operational security policies from some of Australia’s leading organizations. Dilemmas and challenges in developing policies that comply with conflicting laws and regulations were presented to students from the instructor’s prior consulting experiences. Another example was consideration of the advantages and
disadvantages of outsourcing information services to international parties in different legal jurisdictions. Case studies of organizational practice, or malpractice, of security management were presented for students to analyze (Shedden et al. 2010; Ahmad et al. 2012a). Each of these examples was aligned with the three principles outlined in section 2.

<<Table 1 Key Research Papers - intended to build expertise in particular Research Areas>>

Infused into the discussion and debate were key research papers from the security domain. For each lecture topic presented to the students, the instructor nominated a research paper for discussion that students were expected to have read prior to the class (see the list of discussion papers in Table 2). At the end of the lecture, students were given half an hour, within their themed group, to discuss the paper from the perspective of their own theme and from that of the themes of other groups. Subsequently, the instructor would moderate a whole of class discussion by asking one of the groups to summarize the basic content and argument of the paper and then invite each group in turn to critique the paper from their point of view and make observations and insights. These whole of class discussions were limited to periods of 45 minutes, which gave each group approximately 5 to 8 minutes to present their ideas and rebut or build on ideas from other groups.

3.2. Content Design

The Information Security Consulting subject is delivered over three weekends between the first and second semesters of the Australian academic year, typically over June/July. Sessions hours are 10am to 5pm Saturday and Sunday. Each session is broken down into a number of segments where each segment delivers a particular topic from Table 2. Each segment starts with a lecture of approximately one to two hours which is followed by the class discussion as previously mentioned.

The first lecture (topic 1) begins with an overview of the content, assessment tasks, resources and expectations. A brief history of information security is presented with multimedia clips capturing the state of Information Technology thirty years ago and the security challenges of the time. Much of the discussion revolves around the instrumental role of Information Technology in the transformation of society and the evolution of the security problem. This theme is later the subject of a discussion around the research paper as described above (Diffie, 2008). Subsequently, the instructor presents a case study of a critical infrastructure organization in the power industry. The organization faces considerable internal security risk due to its poor information management practices (e.g. leaking blueprints of key infrastructure to private contractors) as well as external threats from international hackers attempting to tunnel through successive firewalls to control its power network and local activists subverting its distributed computing infrastructure at the site of its terminal substations. The scenario serves to highlight the range and complexity of security challenges to the modern organization and sets the scene for the subject's content. Information Security is defined and in terms of its main properties: confidentiality, integrity and availability.

<<Table 2: Information Security Lecture Topics and associated Discussion Papers>>

The second lecture (topic 2) presents a clear set of objectives for information security in the service of organizations. The instructor divides the class into three groups; each group represents a different information security stakeholder – Chief Executive Officers (CEOs), Chief Information Officers (CIOs), and Chief Information Security Officers (CISOs). The groups use Fitzgerald (2007) to study each stakeholder’s viewpoint on information security. Each group then states its perspective on the key security objectives and challenges to the organization. The groups then discuss the difference in each stakeholders’ perspective and expectations (of each other’s role) and the potential for conflict. The lecture then proceeds to profile a range of security threats and attacks to the organization. Students are asked to design formal and informal measures (rather than technical measures) to anticipate and mitigate each scenario.
The next lecture (topic 3) presents international standards and known security frameworks such as the ISO27001 series (ISO/IEC 27001 2005). Students are encouraged to understand how organizations plan and implement security programs using such standards and codes of practice. The usefulness of these methods is strongly critiqued in a discussion using Siponen (2006) and Shedden (2011) that points to the poor implementation of these standards and the lack of resources and expertise available to apply these standards effectively. The instructor then presents principles of security strategy as they apply to organizational infrastructure (see Ahmad et al. 2012b) and draws an analogy between castles and modern network configurations to illustrate the concept of defense-in-depth.

Both perimeter security technologies such as firewalls and VPNs, and technologies on internal lines of defense such as IDS, anti-virus and access control, are then presented to students (topic 4). The focus is on tactical deployment rather than theoretical development, or in other words via a management perspective rather than a technical perspective. The aim is to assist students to understand how these technologies can be combined to support a security strategy. The particular security challenges faced by organization from the increased mobility of information technologies is the topic of discussion (Schultz 2007).

Topic 5, “writing consulting proposals”, covers feasibility, time investment in proposal writing and research, methodologies, team building, the ways and means of costing a proposal, scheduling concerns, quality control, and the politics of bidding for a contract. Samples of completed consulting proposals from leading consulting firms are circulated among students.

The security risk management process (topic 6) is described with emphasis on the risk identification and assessment process. The instructor uses worksheets provided in the OCTAVE-S methodology to show how the various phases of a risk assessment work together and how the outcome can be captured for presentation to senior management. A philosophical debate on the merits of a risk-based approach to security management takes place with the assistance of Parker (2007) and Baskerville (1991).

The problem of leakage of information and knowledge organizations (topic 7) is presented in the context of Resource Based Theory (Grant 1996; 1997; Teece 2009). Leakage can result in the erosion of Valuable, Rare Inimitable and Non-substitutable (VRIN) knowledge which directly influences competitive advantage and may cause damage to reputation, loss of productivity and fines from breaches of confidentiality. Fundamental theory in Knowledge Management is presented along with an interesting study of the dilemmas faced by Knowledge Managers in promoting knowledge flows to drive innovation on the one hand and maintaining confidentiality on the other (Abdul Molok 2010).

In topic 8, students are taken step-by-step through the phases of preparation, detection, containment, eradication and recovery of an incident-handling plan for organizations (SANS n.d.). Each phase is discussed with realistic scenarios that encourage students to acknowledge the broader implications of policy and procedures on organizational productivity, culture and morale. The lack of double-loop learning from incident response in many organizations is the focus of the discussion following the lecture (Ahmad et al. 2012a).

The quality of security policy (topic 9) is a research-oriented topic based on Maynard and Ruighaver (2007). The many dimensions of quality are presented with a case study from the instructor’s own experiences in a major re-drafting of a series of security policies as part of a compliance exercise. The effectiveness of security policy in organizations is the focus of the discussion (Höne & Eloff 2002).

Finally, the instructor concludes the subject content with advanced topics (topic 10) such as need for increased security intelligence to inform risk management. A guest lecture from a former student profiles the life of an information security consultant (topic 11) and ties the knowledge learnt to the consultant’s recent experiences of which some may refer to recent high-profile cases in the media.

3.3. Student Audience

The subject was offered in June/July of 2012 over three weekends in intensive mode. The subject attracted over 30 postgraduate students in 2012. Students were a mix of full-time industry professionals, part-time graduate course-work students, full-time course-work students and a few undergraduates who applied for special permission to participate. In 2012 approximately half the students were students enrolled in the Master of Information Systems degree and the remaining half came from the Master of Engineering, Master
of Information Technology, Master of Business and Information Technology, and Master of Accounting degrees.

Given the diverse student background, the first assessment item was to identify the motivations and backgrounds of students (see section 3.4 Assessment and Table 3). This allowed the instructors to calibrate their expectations and to give feedback to the students about the motivations of others in the class. Additionally, the instructor was able to manage the expectations of the students for the subject based on these responses. The student responses made for an interesting discussion on student expectations and perceptions of information security as a career (see Table 3). For example, some students thought that the potential for information leakage in particular and security incidents in general was likely to increase which indicated a growing market for security professionals. Other students thought that senior management did not take security seriously which indicated a career in security was unlikely to lead further than a middle-management position. Students with a management background felt that their lack of technical knowledge was an impediment to a career in security whereas students with a technical background felt they didn’t have the communication skills to pursue a security consulting or management position. Some students thought the rapidly changing security threat landscape made the security profession unattractive as it was difficult for professionals to maintain a high-level of security expertise over a long-term career.

<<Table 3: Student Motivations and Aspirations>>

3.4. Assessment

There were four components of assessment in the subject. The first component was a short written piece set in the early stages of the subject consisting of no more than two pages in length that queried student expectations and previous exposure to information security. The intent of this assignment was to calibrate the instructors’ expectations. Students were asked to respond to the following questions (see Table 3 for responses):

1. Prior to taking this subject, what did you know about information security?
2. What motivated you to take this subject?
3. What factors have influenced your view of Information Security?
4. Do you see yourself pursuing Information Security as a long-term career? Why or why not?

The second component was divided into two parts both of which were assessed on a group rather than an individual basis. As previously mentioned, the cohort was divided into five groups and each group was assigned one security knowledge area from policy, culture, risk, strategy and security technologies. Each group was asked to deliver a thirty-minute presentation on a research paper assigned by the instructor from their knowledge area (see Table1). Following presentation of the paper, the group was asked to critique the paper for ten minutes given the expertise they acquired in that knowledge area over the length of the subject. At the conclusion of the presentation the instructor then gave the remaining groups ten minutes each to present their points of view on the paper and the subsequent analysis. Credit for comments made by the remaining groups is recognized in assessment component 3.

In the second part of this assessment student groups were asked to write a literature review paper about the challenges their particular knowledge area posed to organizations. The literature review had to incorporate a minimum of five research papers from reputable journals. The instructor designed the assessment criteria around the following principles:

1. How well does the submission demonstrate familiarity with the Knowledge Area and the themes discussed in class?
2. How well does the submission synthesize, integrate and summarize knowledge from the papers to answer the question?
3. What new ideas and avenues of further research are presented?
4. Is the writing style clear and comprehensible?
The third component recognized individual student contributions to discussions. Students received credit for insightful comments made during question-answer sessions after presentations and general comments made during lectures.

Finally, the fourth component asked groups to write a consulting proposal in response to a ‘Request-for-tender’ (see appendix A for the scenario). The instructor posed as a client and was available to answer any questions regarding security services required. The associated project specification asked groups to provide a detailed proposal, including methodology, costing and schedule of work, team profile, previous relevant work history and client list. In addition, there was an expectation that groups would suggest additional services they were capable of providing even though they were not specifically requested. There was also an expectation that groups would refer to industry standards and frameworks and quality management principles. The students were allowed to generate fictional consultants (along with their fictional profiles and previous work experiences for their proposals). Assessment criteria was designed around the following principles:

1. Service Definition: Range and Types of Services Provided
2. Service Methodology: Technical Accuracy and Rigor
3. Project Management: Team structure, Scheduling, Costing, Quality Assurance
4. Presentation of Proposal: Document Structure and Format

4. Feedback

Student Experience Surveys (SES) are administered in the final stages of each subject delivered at the University of Melbourne. Students are asked ten questions (see Figure 1) that include an assessment of the level of intellectual stimulation, co-ordination, usefulness of learning resources, and whether they felt the subject was ‘well-taught’. Each of the questions are ranked on a 5 point scale: strongly disagree (SD), disagree (D), neutral (N), agree (A) and strongly agree (SA). SES are collated and analysed centrally within the University and results are provided to instructors after students receive their marks. For each question, the standard deviation (S.D.) and standard error (Std. Err.) are calculated, as well as the mean (see Figure 1).

The survey results compare favorably against other subjects in the department with only 1 question (Q6) being below the department average and most questions (especially Q1, Q2, Q4, Q5, Q8) being significantly higher than the averages for the department. For Q4, this subject had the highest score within the department². Almost all students agreed that the subject was intellectually stimulating, had been well-coordinated, was supported by useful learning resources and was well-taught (Q1 – Q 4). Almost 60% ‘strongly agreed’ that the subject was intellectually stimulating (Q1) and was well-taught (Q4).

Qualitative comments were requested from students for two questions – “What were the best aspects of this subject?” and “What aspects of this subject do you believe should be improved?” The students praised lecturing staff for their depth of knowledge, enthusiasm and intellectual stimulation. They reported feeling engaged and enthusiastic despite the length of the sessions. For example, one student responded to the question “What is the best aspects of this subject?” with:

“Strong theoretical framework with strong connections to practice”

Another student responded:

“A small class and the interactive nature of the teaching stimulates critical thought. Some of the concepts learnt I was able to relate to the real world which helped in deeper understanding.”

The primary concerns of the students were the very long teaching sessions, the number of assignments and the strict marking.

---

² When measuring the performance of lecturing staff, the University of Melbourne uses only Q4 as the primary indicator of quality. One subject in the department scored 5 on Q4, but was excluded as it only had 2 student responses.
5. Lessons learned and Concluding Comments

5.1. Fostering intellectual excitement and knowledge transfer

The instructors recognized four key factors that played a role in the atmosphere of intellectual excitement and motivation. These were: new concepts and ideas, an increased level of engagement, opportunities for students to make their own discoveries, and knowledge presented in a practical context.

Most students found the concept of risk as an interesting lens with which to view the problem of security in organizations. Students were exposed to the standard risk assessment process as described in the primary textbook (Whitman & Mattord 2011, Ch. 4) to demonstrate how organizational security risks can be systematically and comprehensively mapped and then ranked according to probability and impact. Risk control strategies were also presented to guide deployment of formal, informal and technical controls to avoid, mitigate, and transfer the risk. Student confidence in risk management was tested against the profound criticisms of Parker (2007) and Baskerville (1991) which lead to excited debate and subsequently deeper understanding of flaws in the theory and practice of security management practices. Similarly, there was considerable attention paid to the challenge of information and knowledge leakage in organizations from a theoretical perspective using Resource Based Theory and organizational challenges in influencing handling of information by employees (Shedden et al., 2010). The instructor presented a series of information leakage risks commonly found in organizations as per his prior consulting experiences.

The most powerful motivating force for learning was the competitive spirit amongst teams seeking to ‘champion’ their assigned areas of knowledge. Competition amongst teams fueled a desire for students to become ‘experts’ in their own respective areas whilst developing enough competence in other areas to criticize and comment on the views of other teams authoritatively. In this way, there was a high level of engagement of the student cohort with the teaching material provided in the subject. The seminal papers assigned by the instructor (see Table 1) played a key role in transferring knowledge and developing expertise in each of the knowledge areas. The papers became the basis for stimulating discussion within groups on the arguments, dilemmas, intentions and contributions of each paper. In particular, Schneier’s (2003) explanation of basic security paradigms in chapters 8, 11 and 12 were invaluable in building the basic understanding of strategy and tactics in security. Similarly, Shedden et al. (2010) was a particularly useful multiple case study scenario that allowed for insightful debate about organizations and their conformance to industry standards.

Rather than engage in passive learning where the instructor simply lectures to the student cohort, the subject employed active learning techniques that suggest students learn more when they teach their own peers. Team presentations on research papers, which are accompanied by analyses, stimulated considerable debate and discussion amongst teams. Team esteem and pride played a key role in generating criticism of each other’s presentations and analyses. There were instances where students provided feedback to each other on drawing on the lecture content, papers they had read and also from their own security experiences. In this way students were making their own discoveries and drawing lessons important to them.
Students were more engaged in debate and discussion when knowledge was presented in a practical context such as in scenarios and cases and where there were obvious dilemmas and tradeoffs to consider. In particular, discussion around research papers where the instructor was an author and was involved in the case studies was particularly profound as more in-depth information could be provided than what was available to students from the paper. These were in the areas of secure knowledge management (Shedden et al. 2010), security learning from incident response (Ahmad et al. 2012a), security strategies in organizations (Ahmad et al. 2012b), and policy (Maynard & Ruighaver 2007). Further, the case studies from the research papers as well as those contributed during lectures were also useful in drawing commentary from students. In particular the role-play of CEOs, CIOs, and CISOs using Fitzgerald (2007) brought the conflicting perspectives of stakeholders, their responsibilities and expectations regarding security into view.

Although the subject has been successful in exposing students to a range of methodological knowledge, practical issues and expert opinion, the instructor felt that students were not able to develop skills in ‘security thinking’. Students struggled with the final piece of assessment where they were expected to provide a proposal for an organization’s security issues (see appendix A for assignment specification). Proposals used high-level language, did not address the organization’s security issues directly and did not identify clear deliverables. Service definition was relatively poor and the methodologies described were not tailored to the organization’s needs. In general, students were unable to piece together services, standards, methodologies and practices to form a coherent view and feasible approach. This remains a challenge for the subject.

5.2. Quality of Teaching Resources and Technologies

The Whitman and Mattord (2011) textbook played a key role in the opening phase of the subject to give students basic principles, concepts and general information about information security, which was echoed through the early lectures. In the instructor’s opinion, the textbook is somewhat verbose but generally well-written in plain language that students can understand. There were no complaints regarding the textbook or the associated lecture material. Students found the majority of the selected papers accessible, relevant and useful for generating discussion and debate. However, students required considerable assistance from the instructor to understand Anderson (2001) and Baskerville (1991) as they presented more complex arguments in more sophisticated language.

5.3. Catering for diverse student needs

The subject covered a range of management topics in the areas of policy, risk, culture, strategy and incident response. However, the instructor found students with an Information Systems background were more engaged in discussion around the human dimensions of information security management such as the effectiveness of policy on the development of security culture, ways and means of moderating risky behavior of employees and communication with senior management on security priorities and corresponding investment. Students with a technical background were more engaged with the effective deployment of technologies and assessing risk of attack on organizational infrastructure. In particular, there was considerable interest around protecting organizations from security risks emanating from the use of mobile technologies.

A key challenge in teaching this subject was considering the differing views and background of students with a technical view as opposed to students with a management view. Table 3 shows the difference in motivations and aspirations for these students after the first session, having completed one third of the subject. Students with a technical background were more likely to have had prior exposure to security topics albeit these were likely to be tools rather than techniques. Interestingly there were students in the technical category that felt that lack of management knowledge was an obstacle to a security career and conversely, there were management students that cited a lack of technical knowledge to be an issue for the same reason. Many of the students thought this subject would help them with their present or future job. They expected the subject would help them to engage with security problems and communicate with senior management.

For students with a technical background the instructor focused on the need to complement technical understanding of firewalls, intrusion detection and access controls with risk assessment methods, defensive strategies for selecting and combining controls (e.g. perimeter defense, layering, defense-in-depth). Further,
much of the discussion around technical controls focused on issues that are typically not discussed in IT security subjects such as user acceptance, behavior change and culture.

5.4. Learning cycles of assessment

The first assessment task provided the instructor with insight into the expectations of the student cohort with respect to the subject and their future plans. Students found the second group-based component stimulating and challenging. Most literature reviews and presentations were completed with enthusiasm and with a high degree of competence. However the instructor felt that the difficulty level of these assessments indirectly encouraged the most competent students in each group to take a leading role which resulted in the less competent students doing relatively less work. This disparity in effort among members of a group is not unique to this subject. The instructor was disappointed with student submissions for the final assessment task, the consulting report. Despite providing a specification and numerous briefing sessions on expectations, all groups submitted proposals outlining high-level services without addressing the tender request’s primary concern around knowledge leakage. Further, the proposals did not provide itemized costings and a detailed costing plan despite the instructor pointing out these were needed.

Teaching the subject in intensive mode had its pros and cons. The instructors found their experiences to be consistent with the conclusions of Davies (2006). Students were immersed in the subject content for longer periods at a time than possible in traditional 12-week semesters. Students were able to form strong relationships with other students which assisted in the development of teams and team-oriented activities. Further, although students did have a reduced opportunity to reflect in the intensive format, the instructor thought that the benefits of team-based reflection should be also be considered. However, feedback from the instructor on assignments was a concern. Since the subject was run over three week-end sessions, with a two week break between consecutive sessions, opportunity to discuss feedback to written submissions in class was limited. Research papers submitted at the end of the second session were discussed in the third session. However, feedback to the consulting report submitted at the end of the third session was provided as a separate written response to each team.

5.5. Concluding Comments

From a content perspective, three principles guided the design, development and delivery of this subject. The choice of textbook, lecture topics, selection of discussion papers and assessment tasks were influenced by the first principle, i.e. information security aims to protect the business function of the organization and therefore must be aligned with strategic business management. However, a comparison between the curriculum in this subject and the content in Whitman & Mattord (2011) and other such textbooks shows coverage of information security management issues is still lacking. For example, major topics such as privacy, governance, and laws and ethics are not covered to the same degree as risk, policy and strategy. Regarding the second principle, there are many resources that point out that the security of information in physical and cognitive environments is inadequate. However, the authors found relatively few resources that provided comprehensive guidance on the security of hardcopy information in the physical environment (outside US army field manuals) and even fewer resources discussing the security of conversations and tacit knowledge among personnel. Given the lack of research in this area, there is considerable opportunity for information security researchers to pursue this line of enquiry. Finally, principle 3 was perhaps the easiest to implement. Over the last few decades a large body of information security research has taken a people perspective perhaps due to widespread recognition that poor information security practices, rather than insufficient technical controls, are the primary reason for information security problems. The authors have included a number of research papers in the curriculum that take a people perspective on the information security problem.

There were two key teaching objectives related to delivery of the subject. The first is concerned with the needs of the modern information security management professional and consultant and is captured by the preceding three content objectives. The second relates to the atmosphere and experience of students in the subject. Here there were a number of positive experiences. Firstly, the subject was successful in generating rigorous debate and profound reflection about the key management issues in information security. In particular, the instructors observed a high level of student enthusiasm and argumentation when advocating their respective points of view. Many students engaged in profound reflection and subsequent intellectual
development after being challenged on their views and assumptions. The instructors intend to replicate this experience in all of our teaching, not just those related to security management. Secondly, the students were able to develop reasonable expertise in their particular themed areas and competency in security management in a very short period of time due to the quality of the seminal works and additional readings (see Tables 1 and 2). Thirdly, the case studies and practice-based scenarios gave students an appreciation for the challenges organizations face in applying security management theory and industry standards to everyday practice. In particular, the difference in expectations and the potential for conflict between senior management, security managers, and operations personnel. Fourth, the instructors were pleased with the coverage of the management aspects of security. In particular, the subject managed to provide sufficient technical understanding of security controls for students to appreciate how controls can be deployed at a tactical level.

Although the teaching model worked particularly well for small class sizes, there are concerns that it might not scale well for larger class sizes (e.g. 50 students or more). This is especially concerning as the number of students enrolled in the degrees of MIS and MIT have dramatically increased. Secondly, although teaching this subject in intensive mode over three weekends has a number of benefits such as appeal for part-time students and depth of student involvement in relatively longer eight-hour sessions, there are also a number disadvantages. There are relatively fewer cycles of assessment which means there is less opportunity to provide quality feedback to students on their progress. This was reflected in the Student Experience Surveys (SES) in Q7 “I received valuable feedback on my progress” which received a relatively lower mark of 4.0 compared to the average. A key challenge in this subject was catering for the varied needs of different cohorts of students who either had a technical or managerial background. For example, when discussing how to deploy firewalls to create a defense-in-depth network strategy, students with a management background were not engaged. Similarly, when expounding the benefits of security governance structures, students with technical background were not engaged. Finding a balance between the technological and managerial aspects of security topics was particularly difficult.

The next stage of this research project will focus on the role played by graduates of this subject in industry. Specifically, we intend to examine the influence of our subject on the strategies and methods of our graduates once they are employed as information security consultants. Further studies may seek to generalize by comparing graduates from our subject with consultants without a formal education in information security.

References


Appendix A

MayneSmithDouglas (MSD) is a multinational corporation based in London (UK). MSD manufactures pharmaceutical drugs, plasma products and vaccines as well as consumer health related products. Among these are a range of products for mental health, virus control, diabetes, cancer, influenza and anti-venoms. MSD is widely recognized as one of the top five global companies with a market capitalization of approximately 75 billion pounds. MSD is listed on the FTSE 100 index and has a secondary listing on the New York Stock Exchange. Although MSD is centrally located in the UK, there are a number of facilities in the USA, Canada, Switzerland, France, Belgium, India and Brazil.

Over the last ten years the level of security risk to MSD has risen dramatically for multiple reasons. Much of the workforce of MSD across the world has transitioned from permanent to casual contracts thereby posing new and elevated security risks to MSD trade secrets and production operations. In the previous year alone there were multiple incidents of real or perceived contamination of drugs due to the actions of disgruntled employees. These resulted in significant losses to MSD from having to recall drugs across the world, addressing significant litigation against MSD by alleged victims and efforts to repair damage to the brand and regain market position.

In addition, MSD has experienced incidents of industrial espionage involving some of its top scientists. MSD engaged Pinkerton Consulting and Investigations, a division of Swedish security company Securitas AB to investigate. After a lengthy investigation, Pinkerton has identified the source of these incidents to be a potential competitor based in Eastern Europe looking to replicate MSD drugs for sale at a fraction of the current retail price.

Scope of Services

MSD is requesting a proposal from qualified vendors capable of performing a full and comprehensive information security management review. The review must consider the adequacy of MSD information security strategies, behavioural norms, controls and especially policy given the strong likelihood of future litigation against employees engaging in industrial espionage or other security violations.

Although not all risks have been identified, key security risks relate to the following:

- MSD R&D programs that generate considerable Intellectual Property and Trade Secrets
- MSD information assets such as information about clinical trials, about employees and their identities, and customer lists including orders, volumes and so forth
- MSD IT infrastructure and capability to respond to incidents

As part of the engagement, the Consultant will be expected to provide the following:

- A description of the methodology employed during the assessment
- Clear and concise near, mid, and long-term recommendations regarding security management including, but not limited to:
  - Recommendations for improvements to policies, implementation guidance, and practices to prevent a reoccurrence of vulnerabilities
  - An effective and concise implementation roadmap of the recommendations.

The report must provide an action plan that can be used by MSD to improve the security management program in general. The Consultant will be required to give a formal presentation of their results of the security review to MSD Senior Management. The presentation must be conducted within two weeks after the completion of the services.

In addition to the above, the consultant will be required to provide one session of security awareness training for MSD senior management coupled with education on current security trends and issues relevant to corporations in the Pharmaceuticals Sector. A survey for end users to review the effectiveness of the workshop must also be delivered.
Assignment Specification:
You are required to submit a comprehensive proposal to MSD that addresses their needs and concerns. The proposal shall include, but is not limited to the following:

- The proposed scope of services offered. The minimum scope is indicated in the above section, but you are encouraged to propose additional services that add to the completeness of the consultancy.
- Project team organization.
- Proposed program and schedule indicating the area of work, deliverables and timeline for the review.
- Profiles, qualification and experience of the team to undertake the assignment.
- You must provide a brief write-up on your competencies and experience in review of Information Security management especially policies.

You must:

- State and explain in detail the framework and methodologies to be adopted in this assessment, as well as any industry best practices to be used.
- Submit a list of customers who the Consultant had provided similar services to.
- Submit an outline of the presentation (general topic areas to be covered) during the end-user workshop.