Proceedings of the 14th Colloquium for Information Systems Security Education
Baltimore Marriott Inner Harbor
Baltimore, Maryland June 7 - 9, 2010

Developing a Strategic Security Planning Module for Multidisciplinary Policies Courses

Jeffrey P. Landry, *University of South Alabama*

Abstract – This paper describes an integrative approach for teaching information systems (IS) security issues within an IS strategy and policy course. The educational strategy is to get students involved in thinking critically about information systems (IS) security issues in an executive role. The educational goal is for students to develop an information systems plan, thinking about security issues early—that is, while information systems are in the planning stage—and in concert with the all-too-often compartmentalized topic of ethics. The result is a strategic security planning module. The educational approach is described and outcomes mapped to a pair of accepted information security education standards.

Index terms – information security management, planning, risk assessment, curriculum, outcomes

I. Introduction

An information systems (IS) strategic management course is an excellent place for incorporating information security outcomes. Both strategic management and information security have essential activities that are forward-looking, planning-oriented, and that should be done together. Strategic management for IS establishes a direction for IS in support of a business strategy. Information security management includes risk management for identifying and responding to information-related threats before they occur. This paper's view is that a security strategy should be in place to support an IS strategy, just as an IS strategy should be in alignment with the business [1]. Teaching information security management along with IS planning generates student awareness of the importance of security at the highest levels of the organization—the executive level. Students are taught and get to experience how to think about security like a CIO/CISO. The approach reinforces to students the importance of security issues being treated seriously and proactively by top management.

The purpose of this paper is to provide guidance to IS management educators whose goal is to improve the teaching and learning of information security management in an information systems or management course aimed at learners in multiple disciplines.

Jeffrey P. Landry, University of South Alabama

The remainder of this paper describes the educational approach used. It introduces a framework for integrating information security with information systems strategy and policy course, called strategic security planning. It aligns security-related learning activities with two information security education/training standards [2, 3], and describes the author's development of a strategic security planning assignment. While all or most of the security management topics might be familiar to information security educators, what perhaps is novel about this paper is the integration of security management with strategic IS management course, where the topics are often compartmentalized.

II. Educational Approach

Both the National Centers of Academic Excellence in Information Assurance Education Program [4] and the information security common body of knowledge [5] recognize that information assurance (IA) is a multidisciplinary science taught in various academic programs, including computer science, business administration, information systems management, sociology, and law [6]. This paper describes a multidisciplinary approach used in information systems strategy and policy courses taught at both the graduate and undergraduate levels. Students taking the course major in either business, information systems, information technology, computer science, or engineering. While realizing there are security problems and solutions at different technical layers, for instance database, networks, applications, and operating systems, this course focuses on an executive-level approach. The emphasis is on the business and management issues related to information security, including risk, ethics, legal compliance, and analytical and critical thinking for aspiring professionals with an overall responsibility for organizational security, rather than day-to-day technical responsibilities. The perspective is that information security is a management problem.

The educational approach used to teach information security management is strongly influenced by the guiding assumptions of the information systems profession, from the standpoint of the IS2002 model curriculum [7], the ACM IT Curriculum 2008 [3], and the government's information assurance training standard for

ISBN 1-933510-99-4 ©2010 CISSE

senior systems managers [2]. These assumptions include emphasis on (1) "a broad business and real world perspective", (2) "strong analytical and critical thinking skills," (3) "strong ethical principles…good interpersonal, communication and team skills," and (4) "design and implement IT solutions that enhance organizational performance" [7, p. v]. The assumptions also include recognizing that "security and information assurance have risen sharply in importance in recent years," and that "since protection is only as good as the weakest point in the system…the scope of concern encompasses the total system" [3, p. 20].

III. Integrating Security with Strategic Planning

Integrating information systems planning with security planning, or strategic security planning, seems to be a prudent thing to do, and worth teaching together. Arguably, the IT 2008 model curriculum supports the integration of IT planning and security management. For example, one core outcome calls for "explain(ing)…why information assurance and security must be 'built in' to design and architecture from the beginning to be most effective" while another core outcome would have students "outline the system life-cycle and its relationship to security" [3, p. 77]. Deploying information systems induces immediate security implications: one cannot afford to deploy and only afterwards then start to think about security, as threats would already be crippling the organization. And, because security management requires resources, it is prudent for each new proposed IT project to include the scope, time, and cost estimates for making it secure, so that the fully estimated costs and benefits of projects were available for the selection process.

Textbooks [8] often do not integrate these topics, and so the challenge is on the instructor to integrate them in courses. The goal was to integrate security planning with an already successful information systems strategic planning assignment without excessively increasing student cognitive load in the process of adding the new material.

Table 1 – Selected IT 2008 Outcomes For Strategic Security Planning

IT 2008 ref *(coverage)*	**Outcome**
FA.C.4 *(not covered)*	Explain the security mindset and the role of "paranoia" in that mindset.
FA.C.11 *(somewhat covered)*	Describe a disaster recovery scenario.
OI.C.1 *(fully covered)*	Describe legal and ethical considerations related to the handling and management of enterprise information assets.
A.C.9 *(prereq)*	Identify and distinguish between the different types of Malware (viruses, Trojan horses, worms).

A. Mapping to Outcomes in Model Curricula

From a learning outcomes perspective, the enhanced planning assignment addressed a number of outcomes defined in IT 2008 related to strategic security planning. The result was to modify the strategic planning assignment to include security management, and then add additional homework assignments and exam questions to address learning outcomes. IT 2008 lists 24 outcomes of which 17 are at the core level and 7 at the advanced level. Not all outcomes are covered on the team-based planning assignment. A total of 12 or half of the 24 outcomes were fully or mostly covered by the assignment, five (5) were somewhat covered, and seven were not covered, or considered prerequisite knowledge. See Table 1 for an example of each. Additional assignments and exam items are required to reflect on the team project and assess the additional outcomes. The outcomes covered primarily map to the Function Two –Review Accreditation of the CNSSI No. 4012 standard [2], including topics in the sub-areas of threats, countermeasures, vulnerabilities, and risk management.

B. Engaging Learners in Security Thinking

The first step in developing strategic security planning pedagogy was to introduce and teach security planning. The instructor assigned the chapter covering managing information security to be read, and had students identify and define vocabulary terms for sense making. The instructor then used a constructivist approach to learning. With the constructivist approach, the attempt is to take existing knowledge and frameworks related to the new subject and attempt to reconstruct the new material, with student involvement. The students were asked the question,

What does information systems security have to do with each of the following?

- rational problem-solving
- warfare
- risk management

The three areas were familiar to the instructor and the three populations of students in the course: business, information systems, and engineering majors.

Conceived of as an application of a generic risk-management process, we chose a four-step information security management process. The four-step process is a condensed version of the 9-step risk assessment process defined by the NIST 800-30 [9], a government standard risk management guide which is also referenced by a learning outcome in the IT model curriculum. The four-step process includes:

1 – Identify organizational security threats

2 – Analyze information security threats

3 – Formulate information security policies

4 – Evaluate the security solutions

There is a loop going from step 4 back to the previous steps. This was understood in light of previous problem-solving and risk management models as incorporating a "looking back" or "find new risks," and the warfare metaphor [10], particularly viewing security management as an escalating war in which you cannot totally defeat the enemy, and needing a reconnaissance platoon to evaluate new threats.

IV. Steps of the Security Planning Process

Next, each step had to be more fully developed with guidance and templates. At the same time, the approach had to fit a business-IS strategy planning assignment that had been used in previous semesters without in-depth consideration of security issues. In the IS planning assignment, the students work in teams over 6-8 weeks in a regular semester, using a real or imaginary organization to develop a business strategy, and an aligned IS strategy, down to the level of describing a portfolio of IT projects.

We developed the details of the security planning process as shown below.

A. Identify Organizational Security Threats

Students asked about the sources of security risks, or threats. This is not a trivial issue to consider, because students, although they are familiar with common threats, like viruses and denial of service, might not have an awareness of enough of them, nor have a method to elicit a close-to-complete list. We discussed that threats might be identified multiple ways:

- from a list of common threats
- by first identifying information assets and their importance to the business
- by thinking about the components of an information system that might be vulnerable
- by thinking about people as sources of threats
- by thinking about people as being vulnerable

The threats can be broken down to include both human and environment causes, intentional and unintentional. The chapter on information security management lists common approaches hackers use, including cracking the password, tricking someone, network sniffing, misusing administrative tools, playing middleman, denial of service, Trojan horse, viruses, and spoofing [8]. Additionally, a student question pointed out that people might not follows policies, or they may inadvertently cause accidental harm or loss. In addition, natural disasters, such as fires, floods, earthquake, and tornados are sources of threats.

A means of identifying information assets and their importance to the business was considered, because of the integration with strategic planning. Understanding the business is already part of the project. Another component of the project is to identify and describe potential IT projects as part of the IT strategy. Each IT project would include a description of key information systems components already defined and discussed in the class, including: the technology artifacts—hardware, software, databases, telecommunications and networks—and the two non-technical components—people and procedures.

The instructor suggested that threat identification might proceed in one of two ways, or a combination of both. First, you might identify the various people involved in an enterprise, including their level in the organization or their role, such as the system trinity, and think about how those people might be a source of intentional or accidental harm or loss—how they might be a threat. Or, one might think of the various technical components of an IS, and think about each component as a source of a threat or housing an important information asset. If you identify the components of important systems, then you will therefore identify security-related information.

Arguably, and in accordance with most professional codes of conduct, the most important component of an information system is the people. Therefore, it is important to think of people responsibly, not just as a security threat. So, the students, in accordance with the outcome on social and ethical issues, were asked to think of the people in terms of how they are vulnerable. The following critical questions are relevant:

- Who might be vulnerable?

- What might be vulnerable?
- What legal or ethical responsibility lies with the enterprise management in protecting individuals?
- Think about how to protect each party, in terms of privacy, accuracy, personal and intellectual property, and access.

To guide the students in identifying the actual people to use, the question can be posed to students: How do we identify important people, when we are doing (1) strategic planning (2) security planning, and (3) assessing ethical and legal responsibility?" Two sources were used: (1) a list of power relationships in the extended enterprise, from the linkage analysis planning technique discussed in the course text [8], and (2) a list of published human threat sources [5]. The "strategic" people identified by the linkage analysis technique include internal and external players, including top and middle management, operations, retailers, distributors, suppliers, government, stockholders, competitors, and financial institutions. The "human threat" people include malicious outsider, malicious intruder, (bio)terrorist, saboteur, political spy, corporate spy, lost key personnel, and people making mistakes. A critical question posed to students is "which of the strategic players are possible sources of each human threat?"

A note to make about the fourth point above is that to generate the ethical questions, the course coverage of computer ethics [8], the Mason's PAPA article [11] and a book on computer ethics [12] were consulted. As an additional critical thinking activity the students could be asked to compare and contrast the property, accuracy, property, and access issues with the security principles [22] of confidentiality, integrity, and availability that can be argued to be similar or overlapping. This additional thinking exercise would get students thinking about justification for students to adopt a strong, ethically-based approach to security management.

B. Analyze Information Security Threats

Following a risk assessment approach, this step involved calculating the probability and severity of each threat. Either qualitative (high, medium, low) or quantitative (probability from 0 to 100%, severity from 1 to 5) are possible. In a student planning assignment, such estimates would probably be a rough, shot-in-the-dark estimate and difficult to defend. The instructor found and adapted a source [5] that provided various items to help focus in on each dimension. For threat probability, the items include skill, ease of access, incentive, and resources, and use a 1 to 5 summative scale. Threat severity is represented as five levels (insignificant, minor, moderate, major, and catastrophic) based on business impact and loss of confidence.

C. Formulate Information Security Policies

Students were required to describe policies to address the most serious threats, and go into detail on one of them, while weighing the most important ethical dilemma presented by their security policy. Guidance on this task came from four areas: (1) the list of management and technical countermeasures provided in the course textbook [8], (2) specifically using the knowledge of information assets and people/roles previously identified to establish access and use policies, (3) consideration of the possible responses to risk: mitigation, avoidance, transfer, and acceptance, and (4) using the warfare metaphor (i.e. defend the castle, reconnaissance platoon, wear your amour, war room, stop the bleeding, etc.) to craft an IT security battle plan. A key issue that arose during class discussion was on the subject of consequences of non-compliance of policy. "What if the people do not follow the policy?" was the question. Guidance given includes the components of a written policy, including sections such as title, objective, purpose, audience, policy, exceptions, and disciplinary actions [13].

D. Evaluate the Security Solutions

The evaluation step differs from professional practice. Given that we are not actually going to implement our plans, the nature of assessment has to focus on the quality of the plan rather than on the effectiveness of the implemented solution.

Following the outcomes-based, learner-centered approaches used, the planning assignment is linked to multiple course outcomes, and assessment criteria, and rubrics are provided a priori, providing instruction and guidance as well as assessment. The assignments are also submitted and feedback provided in multiple—two to three—drafts. In the past, this has been effective at reducing grading anxiety while steering them to value performance based on outcomes-achievement. The teams are used as discussants; each team is given a draft plan of another team and asked to provide constructive feedback, guided by the outcomes and rubric. The instructor independently assesses.

An evaluation rubric for the information security and ethics related outcomes in the strategic security planning assignment appears as an appendix to this paper.

V. RESULTS

In the fall of 2009, the approach presented in this paper was used in a management information systems course at

the author's university. The course was a required course in two graduate programs, the MBA and Information Systems masters programs, and for the current term, six undergraduate students of the class of 52 attended to satisfy their prerequisite requirement for an IS strategy and policy course. The instructor split the class into 13 project teams, two of which were 3-member undergraduate teams. The remaining 11 teams had at least one member each from both the MBA and IS Master's programs. The teams developed an information systems plan with integrated security plan for a chosen organization in various industries. The organizations chosen included:

- Children and women's hospital
- International hotel chain
- Cardiologist physicians clinic
- Online travel agency
- Real estate agency
- US Dept of Health and Human Services
- Large airline
- Chemical plant
- Hotel chain
- Public high school
- Advertising agency
- Snack food vendor
- Home improvement retail chain

The following strengths and weaknesses ("could be better if…") were summarized from feedback on the 13 projects. The strengths and weaknesses come directly from written feedback provided by the instructor and discussant teams.

- "solid security planning"
- "you included the pertinent legal issue (HIPAA compliance) along with social and ethical issues"
- "a myriad of social and ethical issues identified and concisely described across all four PAPA categories"
- "a well-written social and ethical issue analysis that tied in legal compliance"
- "bonus for social/ethic consequences, not so much because of the quality of the particular section of the report, but because you overall plan is effective at dealing with one of the most—if not THE most—pressing social and ethical issues of our day" referring to the team that chose the US Dept of HHS and national health care and EHR.
- "solid security plan; good job of prioritizing ethical issues using PAPA as framework, as privacy rose to the top"
- "informative ethical scenarios empathetic to student (children's) point of view" for the public high school team
- "mutiple ethical issues identified, with stimulating scenarios described"
- "thoughtful ethical analysis"

Feedback on weaknesses included, "could be better if…"

- "you had used the PAPA framework for social and ethical issues, and if you had been gone deeper; for example, listing 'this could lead to lawsuits' in several places is not clear. What laws, for example, would be violated by what particular kinds of actions? Who would be legally responsible, according to your analysis? You did not break your analysis down by PAPA at all, it seems; some dimensions are still vague in security and ethical section"
- "you had gone deeper in one of the social/ethical issues, and had identified outcomes, both positive and negative; it looks like what you did was to describe what the hotel believes to be its ethical responsibilities, rather than what you were supposed to do, which is 'identifying and critically evaluating the ethical, social, and legal consequences of your strategic IS plan'"
- "your security plan had one policy going in-depth; while you mentioned security within a couple of the projects, there is no actual risk analysis process described. We discussed this and understand it is in work. Ensure that you identify, assess, mitigate and then re-assess the risks involved in your business"
- "you had prioritized security threats"
- "Numerous security issues were handled. Networks/equipment failures can also be considered as threats; you had addressed some of the key ethical issues in real estate, including the issues of disclosure of information about homes, including what's wrong with them, the issue of representation (buyer vs. seller, and any of the regulatory issues you mention"
- "you had identified positive outcomes and who benefits"
- "you would go deeper in one of the social/ethical issues"
- "the social and ethical issues section had reflected better reflected the magnitude of these issues that your plan otherwise took head-on"
- "you identified PAPA issues, and specified which parties would benefit"
- "you added more security measures for theft, burglary and auto theft by installing more cameras and adding security personnel and monitoring all hotel properties through centralized system similar to ADT or Brinks (now known as Broadview) security."
- "you had explained further why each of the threats were assigned such priorities, going into more depth about resolving issues"
- "you would clarify security threat countermeasures"
- "you had mentioned encryption as an additional countermeasure to thwart the ethical/security issue of accessibility"

Overall, teams did a good job when they applied the step-by-step security planning process, when they identified

many threats, not missing any, when they described these threats and countermeasures well, when they used helpful frameworks like threat source lists and the Mason's PAPA categories, when they hit the most important security/ethical issue for that organization and industry, and when thoughtful ethical scenarios showed awareness of and concern for the ethical implications of their plans. Teams did not do as well, when they did not demonstrate that a logical assessment process was being used, when they did not prioritize, when the left out glaringly important threats or countermeasures, or when the descriptions were vague.

The discussant teams caught issues that the instructor did not. The use of frameworks, such as common threat lists, threat sources, such as the ones in NIST 800-30, and the PAPA categories for ethical issues were all helpful in guiding the students and assisting the instructor and discussant teams.

Areas for improvement include two suggestions. Have students do more research into risks in their industry and technology domains pertinent to their organization. Improve the means of evaluating threat identification. Like Dykstra's notion of the difficulty (or impossibility) of proving that software is correct, it is also difficultly to prove that no high-risk threats are missing. Such as process or guideline would be helpful to both the teams, instructor, and discussant group. Clearly, the use of categories is helpful, along with multiple levels of review.

VI. Conclusions

The strengths of the strategic security planning approach are that it is supports government [2], and academic [3] curriculum guidelines, addresses an important top management perspective on security, and is accessible to both technical and non-technical students in different majors. The coverage maps into some but not all security-related outcomes identified in the IT curriculum model. This approach was not argued to be a comprehensive approach to security education, however, and there are other areas in the curriculum to cover security from additional perspectives. However, the strategic security planning module did manage to address as many as 17 of the 24 learning outcomes in information security.

VII. References

[1] D. L. Pipkin, "Linking Business Objectives and Security Directives," in Whitman, M. E. and Mattord, H. J. , Readings and Cases in the Management of Information Security, Thompson Course Technology, Boston, MA, 2006, p. 11.

[2] Committee on National Security Systems—CNSS (2004, June). National Information Assurance Training Standard for Senior System Managers: CNSSI No. 4012. National Security Agency. Available from http://www.cnss.gov/Assets/pdf/cnssi_4012.pdf

[3] Lunt, Barry M., et al, Information Technology 2008 Curriculum Guidelines for Undergraduate Degree Programs in Information Technology, Association for Computing Machinery (ACM), IEEE Computer Society, November 2008, Available from http://www.acm.org/education/curricula/IT2008%20Curriculum.pdf/view

[4] Centers of Academic Excellence, National Security Agency, URL: http://www.nsa.gov/ia/academia/caeiae.cfm, accessed on June 17, 2008.

[5] Tipton, H. F. and Henry, K., Official (ISC)^2 Guide to the CISSP CBK, Auerbach Publications: Taylor and Francis Group, Boca Raton, FL, 2007.

[6] M. Theoharidou and D. Gritzalis, "Common Body of Knowledge for Information Security," IEEE Security & Privacy, vol. 5, no. 2, IEEE, Inc., March/April 2007, pp. 64-67.

[7] Gorgone, J. T., Davis, G. B., Valacich, J. S., Topi, H., Feinstein, D. L., and Longenecker, H. E. Jr., IS 2002 Model Curriculum and Guidelines for Undergraduate Degree Programs in Information Systems, ACM, New York, NY, AIS, and AITP (formerly DPMA), Park Ridge, IL, 2002, pp. 6-7.

[8] McNurlin, B. C., Sprague, R. H. Jr., and Bui, Tung, Information Systems Management in Practice, Eighth Edition, Pearson Prentice Hall, Upper Saddle River, NJ, 2009.

[9] G. Stoneburner, A. Goguen, and A. Feringa, "Risk management guide for information technology systems: Recommendations of the National Institute of Standards and Technology." Gaithersburg, Md: U.S. Dept. of Commerce, National Institute of Standards and Technology, 2002, http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

[10] M. E. Whitman, and H. J. Mattord, "Zen and the Art of Information Systems Security—A Philosophical, Spiritual, and Mystical Approach to Protecting Information," in Whittman and Mattord, Readings and Cases in the Management of Information Security, Thompson Course Technology, Boston, MA, 2006, pp. 33-44.

[11] R. O. Mason, "Four Ethical Issues for the Information Age," MISQ Archives. Management Information Systems Quarterly, 10:1, March, 1986.

[12] Quinn, M. J., Ethics for the Information Age, Pearson Addison Wesley, Boston, MA, 2005, p. 380.

[13] Greene, S. S., Security Policies and Procedures: Principles and Practices, Pearson Prentice Hall, Upper Saddle River, NJ, 2006, pp. 98-99.

Table 2 - Security and Ethics Evaluation Rubric for Strategic Security Planning Assignment

Outcome Success Criterion	Assessment Scoring
O7-Developing and evaluating information security policies that identify, assess and resolve important security threats to your enterprise	summary of multiple dimensions listed below
- Using a rational, risk management oriented security planning process?	security threats were: 1-identified 2-identified & assessed 3-identified, assessed & resolved
- Were important threats missed?	threat(s) missed were 0-catastrophic 1-major 2-moderate 3-minor 4-insignificant
- Were threat prioritizations accurate?	1 - underestimated a major or catastrophic threat 2 - overestimated a minor or insignificant threat 3 - prioritized threats accurately
- Were policies complete?	2-superficial policies for top-3 threats 4-adequately explained policies for top-3 threats 6-at least one policy goes in-depth
- Effectiveness of the in-depth security policy at resolving the threat	very ineffective 1 2 3 4 very effective
O9-Identifying and critically evaluating the ethical, social and legal consequences of your strategic IS plan	summary of multiple dimensions listed below, multiplied times 2
- For the PAPA issues, - Were most important issues in each area addressed?	0-two or more PAPA categories missing big issue, 1-only one area missing big issue, 2-each area has a big issue identified
- For the ethical issue analyzed in-depth… o Was there a more important issue to be addressed?	1-ethical issue they identified was trivial compared to what they did not cover, 2-they covered something important, but missed something bigger, 3-they covered the most important issue
o Were those who benefitted or were harmed identified?	0-no parties identified 1-vague reference to an affected party, 2-specific parties (individuals, groups, business partners) were identified
o Were outcomes described and assessed?	1-only one outcome, 2-both good and bad outcomes identified, 3-outcomes identified are well-explained and assessed