Planning Organizational Security: The Health First Case Study

Susan J. Lincke
University of Wisconsin-Parkside
900 Wood Road
Kenosha WI 53141 USA
+1(708)453-2069
lincke@uwp.edu

ABSTRACT

Security is important skill for an IT professional, and allows him/her to advance and specialize in their career. We developed an Information Security course with a goal of training students for the ISACA CISA and CISM exams, and having students participate in security planning with not-for-profit organizations. The Health First Case Study enables students to practice security planning with a hypothetical Doctor's office, including risk analysis, business continuity, information security, network security, personnel security, incident response, and physical security. Students use the Small Business Security Workbook, which leads them through the security planning process. The case study also helps students to understand the perspective of the business owner.

Categories and Subject Descriptors

K.3.2 Information Systems Education; K.6.5 Security and Protection

General Terms

Security, Management.

Keywords

Security Planning, IT, Security Workbook, Case Study.

1. INTRODUCTION

This NSF-funded project has developed lecture materials and a hypothetical case study, based on a doctor's office, to help students plan security. Students use the Small Business Security Workbook to guide them through the security planning process. They practice with the Health First Case Study, and then optionally work with real organizations, as part of community-based learning.

We developed our Information Security course from professional security materials. These materials are based on ISACA's Certified Information Systems Auditor (CISA) and Certified Information Security Manager (CISM) review manuals [1,2]. These materials discuss security from a high-level, business perspective. This knowledge compliments the Security+ certification, which emphasizes secure computer operations. The CISA/CISM help to train security analysts, while the CompTIA Security+ certifications help to train security administrators [3]. The CISA or CISM focus on aspects covered by the CISSP certification, and thus can serve as a spring board to eventual CISSP certification [4].

This course is an elective for our Computer Science and Management Information Systems majors, and a required course for our graduate Computer Information Systems program. This course is most useful as an upper level undergraduate or a graduate IS/IT/CS program.

We developed this course with a case study, to provide an active-learning or problem-based learning experience. Lu and Wang [5] found that case studies enable student-centered learning, by promoting interactivity between students and faculty, reinforcing educational concepts taught by lecture, and deepening student understanding by building knowledge into students. Students not only learn to apply theoretical knowledge to practical problems, but also to be creative in discovering solutions.

Our case study was meant to provide students real world experience in security planning. Wei et al. [6] found that cases help students transition to the workplace, by exposing students to diverse situations, thereby enhancing adaptation skills to new environments, and increasing students' self confidence in dealing with the world. Students increase their communications skills, which includes listening and persuasion skills.

We did not expect, but found that our case study exposes students to multiple views. Chinowsky and Robinson [7] stress that case studies enable interdisciplinary experience, which students are more likely to encounter in the real world. They stress the importance of using real-world artifacts in the case study. Our case study achieves the interdisciplinary aspect, by enabling students to experience multiple perspectives: the doctors', HIPAA regulation, IT and financial, including through the use of real artifacts: business documents.

We are aware of four sets of case studies relating to security. Dhillon [8] has written a security text that describes a company's basic scenario as an introduction to each chapter. At the end of each chapter is a case study problem, which has students consider specific aspects related to the case study. ISACA also provides graduate-level teaching cases [9,10], which emphasize corporate governance problems related to security management and the

Conference'10, Month 1–2, 2010, City, State, Country.

COBIT maturity model. However, understanding law, in addition to security technology, is also important for IS security students [11,12]. Schembari has students debate legal case studies, to help them learn about security-related law [12].

In this case study, students plan security for a doctor's office, which must adhere to the U.S. Health Insurance Portability and Accountability Act (HIPAA). Through this law, students understand that security procedures are important, including risk, business continuity, physical security, and personnel security. HIPAA is important in the U.S., because approximately 58% of organizations must adhere to it, and it is representative of regulation that is concerned with state-of-the-art privacy and security. While these teaching materials are freely available, some aspects of the case study will need to be modified for use in other countries to reflect national law. Nearly all of the lecture materials and the Small Business Security Workbook can be used in other countries without modification.

This paper describes an introduction to our course, our IT-related case studies, notes on teaching with the case study, our results, and a conclusion.

2. THE INFORMATION SECURITY COURSE MATERIALS

The Health First Case Study can be used for a semester long course. It is one case study in that it addresses one business: a doctor's office. However, it is a collection of case studies, since each case study develops some aspect of the security plan. The case studies can be used as active learning exercises or homework assignments, after each lecture.

Students make important decisions regarding the security planning process. The case study is provided as conversations between the doctor and staff, and an IT person. The Small Business Security Workbook leads students through the security planning process. The Workbook has been tested with real small businesses, via service learning [13]. Other aspects of the full case study investigate secure software development, working with HIPAA [14], and technical network security (including protocol analysis) [15]. The case studies described here are IT-related, and used for security planning.

Each case study is associated with a PowerPoint lecture, which includes sample Workbook tables for a scenario related to a university.

2.1 Case Study Exercises

The Health First Case Study addresses seven areas in IT: 1) risk management, 2) business impact analysis and business continuity, 3) information security, 4) network security, 5) physical security, 6) incident response, and 7) personnel security. For each of the case studies described below, the students refer to the lecture and Workbook to complete each exercise. The case study exercises include:

2.1.1 *Analyzing Risk*

This case study is performed after the Risk Management lecture. Students first determine the value of the assets and list the probable threats for the doctor's office. Students work with real business documents, including an Income Statement, Statement of Retained Earnings, and a Balance Sheet. HIPAA jail sentences and financial penalties increase the cost of security breaches, and factor heavily into the risk analysis process. Students then complete the remaining risk analysis steps of: estimate likelihood, compute expected loss, and treat risk. Table 1 shows a partial result of the treat risk process.

The outcome for the business is a risk analysis plan within the Workbook. Learning outcomes include working with qualitative and quantitative risk analysis, using real business documents.

2.1.2 *Addressing Business Impact Analysis & Business Continuity*

For a Business Impact Analysis (BIA) plan, students first define potential threats that could severely impact the business. Students then define the business recovery objectives, including the Recovery Time Objective and Recovery Point Objective.

Students then allocate a Criticality Classification to each information asset, and define security controls to address the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for critical services.

The outcome for the business, and the student learning outcomes, is the development of a Business Impact Analysis and the start of a Business Continuity Plan. A complete Business Continuity Plan would include detailed Procedures for Handling, which is not part of the case study.

2.1.3 *Designing Information Security*

The case study has students classify organizational data by Sensitivity (secrecy) and Criticality (reliability). They then discuss how the data should be protected: e.g., for which data classifications should data at rest be encrypted, and how labeled? (See Table 2.) They define organizational roles and define which roles shall have access to which data. With role-based access control, students consider who should be have read/write/execute permissions to the various forms of the Health First database.

Table 1. Analysis of Risk versus Controls

Risk	ALE Score	Control	Cost of Control
Malpractice	$50K	Medical server up	
Social Engineering	$25K	Awareness training HIPAA Adherence	Weekly HIPAA meetings, Annual training
Stolen Information/ HIPAA audit	$15K	HIPAA Adherence, Encrypted disks, VPN, firewalls, antivirus software, Audit tech/service	Weekly HIPAA meetings, Encryption & security technology

Table 2. Handling of Sensitive Data

	Confidential	Privileged
Access	Need to know	Need to know
Paper Storage	Locked cabinet, Locked room if unattended	Locked cabinet Locked room if unattended
Disk Storage	Server-only storage Password-protected, Encrypted, Hashed	Password-Protected
Labeling & Handling	'Confidential' Clean desk, low voice, shut doors	Clean desk
Transmission	Encrypted	Local only, Encr.
Archive	Encrypted	
Disposal	Degauss & damage disks Shred paper	Reformat disks

2.1.4 Planning for Network Security

For this case study, students consider which applications can be stored together on physical or virtual machines, based on access control and Criticality classification. Next, students determine which services are allowed to enter and leave the network, and in which direction those connections should originate. This information is important in configuring the firewall(s). Based on the Criticality and Sensitivity classifications, students then define the required specific controls for each service (e.g., encryption, hashing, anti-virus). Firewalls need to protect the organization's data from both the internet and wireless access!

Finally, students draw a network map for Health First with Microsoft Visio, and color code the different systems according to their Sensitivity Classification. See Figure 1.

The outcome for the business is a network security plan within the Workbook. Learning outcomes include documenting the requirements for a circuit-level firewall, and organizing data by Criticality/Sensitivity classification and role-based access control.

2.1.5 Designing Physical Security

The lecture on Physical and Personnel Security are combined, since they are somewhat shorter than other lectures.

For this case study, room classifications are defined for Sensitivity and Criticality, according to room contents. Appropriate room controls are defined for each classification, including procedural and other physical access and availability controls (e.g., locks, fire suppressant, UPS, etc.) See Table 3. Students prepare a map showing room sensitivity and criticality classifications for Health First.

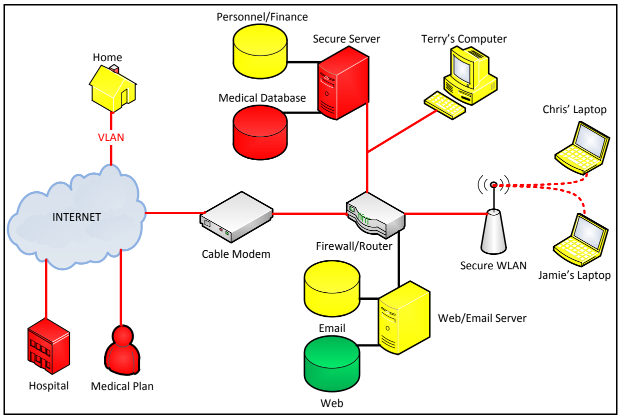

Figure 1. Color-coded Network Diagram

Table 3. Room Classifications

Sensitivity Class	Description	Special Treatment (Controls related to Confidentiality)
Proprietary	Room contains Propriety information storage	N/A
Confiden-tial	Room contains Confidential information storage	Workstation monitor has hood. All cabinets remained locked. Room remains locked when not attended. No patients are allowed in these areas.
Private	Room contains computer with access to sensitive or confidential data	Laptops are physically secured using cable locking system. Room remains closed when unattended, since locks are not in place. Building remains locked when unattended. All cabinets remained locked. No patients are allowed in these areas.
Privileged	Room contains computer with access to sensitive or confidential data but public has access when escorted	Laptops are physically secured using cable locking system. Room remains closed when unattended, since locks are not in place. Building remains locked when unattended. All cabinets remained locked.
Public	The public is free to spend time in this room, without escort.	Room remains open. Building remains locked when unattended. No computers or confidential papers left in room.

The outcome for the business is a physical security plan. The student learning outcomes include a consideration for physical controls for both access and availability.

2.1.6 Planning for Incident Response

This lecture reviews six stages of incident response: Preparation, Identification, Containment, Analysis and Eradication, Recovery, and Lessons Learned.

This case study addresses Stage 1 Preparation, which prepares an organization for an incident (i.e., the remaining incident response stages). This case study leads students to define potential incidents, and their detection mechanisms or controls to limit their occurrence. Suggested incidents include hacker intrusion, lost laptop or backup tape, social engineering, and theft of proprietary information.

Students next address what should happen in the remaining incident response stages, including who should be notified, and what actions need to be taken. Students define which procedures need to be developed, without developing full procedures.

The outcome for the business is an Incident Response Plan, including a list of threats and detection mechanisms, and a definition of actions for when incidents occur. Learning outcomes include students developing appropriate responses for each of the incident response stages, and exposure to the breach notification law (valid for most states in the United States).

2.1.7 Organizing Personnel Security

The Personnel Security is an advanced case study, which requires students have a good understanding of the full information security picture, since they will be allocating security responsibilities to each employee. The Personnel Security lecture describes personnel security issues dealing with hiring/termination, different forms of security training, and segregation of duties.

This case study problem first defines internal threats from fraud for each employee, and then discusses possible controls for each threat. HIPAA requires that organizations define a Chief Security Officer (CSO). During the case study students review the HIPAA Security Rule to allocate responsibility to the CSO and other employees to ensure adherence to HIPAA. Finally, the Workbook has students define the training and procedures that will enable everyone to complete their security-related responsibilities.

The outcome for the business is a coherent system of security, including allocation of security responsibilities, training, and documentation. Learning outcomes include that students evaluate security from the personnel perspective, consider security as a system, work with security regulation, and review previous exercises.

3. NOTES ON TEACHING THE CASE STUDY

The NSF-funded case study materials include PowerPoint lectures, case study, Small Business Security Workbook, and Small Business Requirements Document (with Health First forms). There is also a Small Business Security Workbook Solution, which includes a solution for the full case study.

The lectures have been enhanced to include appropriate example tables from the Small Business Security Workbook, for a University application. These examples help students to observe how tables are properly used, and may provide ideas for their solution (or not!) The lecture notes are made available to students from the course web page during the case study exercise, and they are often referred to.

We teach the case study as an active learning exercise in class, although it could be used as homework. A PowerPoint lecture is given in the first half of a 3-hour class, and the second half is the active learning exercise. For active learning, students are grouped into 3-4 person teams, and each team is provided a computer to edit the Small Business Security Workbook directly on-line. All students should be able to see the display, so computers are selected and manipulated for the best display. The best computers tend to be the ones at the end of a row of tables, providing 3 sides for students to sit, discuss, and observe Workbook use.

The instructor provides a copy per student, of the 2-3 pages of the specific case study exercise. The beginning of each case study indicates the corresponding section in the Workbook to work with, but is also announced by the instructor. The case study has headings to indicate the conversations for each subsection of the appropriate chapter in the Workbook. The Workbook is retained on the computer, so that students may add to the Workbook each week. This enables students to review previous decisions during case study exercises.

The application of the HIPAA regulation is important for this business case. It is important that the HIPAA lecture (or appropriate alternative regulation lecture) is given before some case study exercises. The HIPAA lecture notes are made available to students when necessary. One hard copy of the HIPAA lecture is provided for each group. The HIPAA lecture copies are distributed at the beginning of appropriate labs, and retained for reference in the teaching lab.

The best way to start the case study is to have students volunteer to read the first part of the case study out loud in front of the whole class. Each role is read by a different student. Most case studies have 4 roles, so there would normally be 4 readers. A benefit is that it starts out the case study with students actively talking, and not silently reading (or being confused). Then the instructor can provide direction for class discussion, and get initial ideas into play before letting the groups go off on their own. Assigning roles in each group has the advantage that students get to play a different role each week, including an IT person, versus a doctor or medical administrator.

While the case study is being actively discussed per group, the instructor may see that some groups are too quiet or heading in the wrong direction. It is advantageous to correct this. Rarely, it may make sense to move people between groups, if some groups are not making sufficient progress or not getting along. At the end of the class, the instructor can ask specific teams for their solutions, particularly if they had brilliant ideas that should be shared, and/or can discuss the solution provided by this case study.

As an active learning exercise, students are given a small amount of credit for participating. If students miss the active learning exercise, they can submit it as homework. Due to time constraints, perfect solutions may not occur during the lab time. However, having students think about the solution, and observe a good solution, helps them to assimilate the material. Often students come up with brilliant ideas, which have been incorporated into the official solution!

4. RESULTS

There are two questions when a course is taught: is the teaching effective, and do students appreciate their learning?

The real test of whether the teaching effectively "helps students transition to the workplace", is whether students can work with a community partner on a real project afterwards. After a trial run with the case study, undergraduate students used the Workbook to work with small business management in our community. The instructor led the students for one visit to the community partner if students had IS/IT experience, or participated twice (of 6 visits) if they had no experience. The semester's work was rated highly by the community and students. Of our five community partner organizations that used this Workbook with student guidance, 100% were Very Satisfied with "The Quality of Students' Work". During our last year, students agreed (100%) or strongly agreed (28.6%) with the statement: "I felt that the community project I did through this course benefited the community partner's organization."

To obtain feedback from students about their learning, an independent evaluator performed a qualitative assessment with the students at the end of the course. The consensus on the case study was: "It was a good test drive". "Gave you a guideline for working with your partner". However, there was also a consensus that 'catching on' in the first few labs was difficult.

We also noticed that later labs had higher approval ratings than earlier labs. Our first four labs had an average 78% agreement rate to the statement: "I understood what was expected as part of the case study exercise, and it helped me to learn the material." During the next six labs this rate increased to 87.5%. (In both cases, all remaining students selected "Neither agree nor disagree".) To fix this, we start the case study as a class (and not in separate groups). Volunteers read the case study out loud and discussion begins class-wide. Our initial approval rating then started out higher, with 93% 'agreeing' with the statement: "I understood what was expected as part of the case study exercise, and it helped me to learn the material."

An unexpected benefit noticed by the instructor was that students experience the perspective of the business owner. Students learn that a solution is not just about technology – it is also about the business. Business and technology costs are provided for students to work with, including business financial reports.

5. ACKNOWLEDGMENT

The development of the Small Business Security Workbook, lecture materials, and Health First Case Study was funded by the National Science Foundation (NSF) Course, Curriculum and Laboratory Improvement (CCLI) grant 0837574: Information Security: Audit, Case Study, and Service Learning. These materials are available at: www.cs.uwp.edu/staff/lincke/infosec. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the NSF.

6. CONCLUSION

This case study teaches students to plan for security in IT. Students gain practice with the case study, as for a real-world experience. Students learn to work with the Small Business Security Workbook, which they can use in their workplace, after they graduate.

The case study also achieves an interdisciplinary aspect, by enabling students to experience multiple perspectives: the doctors', regulation, IT, and financial. It is effective, in that students can lead real world community partners through security design.

7. REFERENCES

[1] ISACA. 2009. *CISA Review Manual 2010*. Arlington Heights IL, DOI=http://www.itgovernance.co.uk/products/1403.

[2] ISACA. 2009. *CISM Review Manual 2010*. Arlington Heights IL. DOI=http://www.itgovernance.co.uk/products/1402.

[3] Farwood. 2012. Security+ Guide to Network Security Fundamentals, 4th Ed. CENGAGE Learning.

[4] Harris, S. 2010. *CISSP All-in-One Exam Guide, 5th Ed*. McGraw-Hill, NY.

[5] Lu, S. and Wang, Y. 2009. "The Research and Practice of Case Teaching Method in Computer Curricula for Undergraduates". *Proc. 2009 4th International Conf. on Computer Science and Education*. IEEE, 1460-1463.

[6] Wei, H., Xin, C., and Ying, H. 2010. "Non-computer Professional IT Education in the MBA Model". *The 5th International Conf. on Computer Science & Education*. IEEE, 612-614.

[7] Chinowsky, P. S., and Robinson, J. 1995. "Facilitating Interdisciplinary Design Education Through Case Histories". *1995 IEEE Frontiers in Education Conf.* IEEE, 4a3.6-4a3-9.

[8] Dhillon, G. 2007. *Principles of Information Systems Security*, John Wiley & Sons, Inc.

[9] ITGI. 2007. *IT Governance Using COBIT® and Val IT: Student Book, 2nd Ed.* IT Governance Institute, **www.isaca.org**, Rolling Meadows, IL.

[10] ISACA. 2010. *Information Security Using the CISM® Review Manual and BMISTM: Caselets*. **www.isaca.org**, Rolling Meadows, IL.

[11] Katerinsky, A., Rao, H. R., and Upadhyaya, S. 2010. "Harsh Realities 101 - Augmenting Information Assurance with Legal Curricula". *Proc. 14th Colloquium for Information Systems Security Education (CISSE)*. **www.cisse.info**.

[12] Schembari, N. P. 2010. "An Active Learning Approach for Coursework in Information Assurance Ethics and Law". *Proc. 14th Colloquium for Information Systems Security Education (CISSE)*. **www.cisse.info**, 1-8.

[13] Burri, T. and Lincke, S. J. "Security planning for small businesses: A service-learning course". *IEEE Frontiers in Education Conference (FIE)*. IEEE. Oct. 12-15, 2011, pp. F1E-1 - F1E-6.

[14] Lincke, S. J. 2012. "The Health First Case Study: Teaching HIPAA Regulation with Security". *Colloquium for Information Systems Security Education (CISSE).* June 13-15.

[15] Lincke, S. J. 2012. "Network Security: A Case Study". *Midwest Instruction and Computing Symposium*. April 13-14.

Take care of reference numbering [1] then submit.

Columns on Last Page Should Be Made As Close As Possible to Equal Length