Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2012 Proceedings

Proceedings

Combating IS Fraud: A Teaching Case Study

Susan Lincke
University of Wisconsin-Parkside, Kenosha, WI, United States., lincke@uwp.edu

David Green
Governors State University, University Park, IL, United States., dgreen@govst.edu

Combating IS Fraud: A Teaching Case Study

Susan J. Lincke
University of Wisconsin-Parkside
lincke@uwp.edu

David T. Green
Governors State University
dgreen@govst.edu

ABSTRACT

People are becoming more creative in use of classic fraud schemes via information systems. This paper presents a case study resource for teaching information security controls to help combat information systems fraud. The Health First Case Study is designed to give undergraduate computer science, information systems, and information technology students an opportunity to plan security for a doctor's office, with the guidance of another useful resource, the Small Business Security Workbook. The case study addresses social engineering, ethics, requirements documentation, security design, incident response, and personnel security. Course implementation examples are included for both face-to-face and online courses.

Keywords

Teaching case, security, fraud, small business, health IT

INTRODUCTION

Fraud is not a new phenomenon, and many organizations use internal accounting controls as an attempt identify and prevent fraud. Small businesses are disproportionately harmed by fraud because of the lack of anti-fraud controls compared to larger organizations, making them vulnerable to fraud (Association of Certified Fraud Examiners, 2010) In addition, people are becoming more creative in use of classic fraud schemes through use of computer networks (Panko, 2010) (i.e., information systems fraud).

This paper presents a case study resource for teaching information security controls to help combat information systems fraud. Wei et al. (Wei et al., 2010) write that business case studies can help student learning because they "constitute the basis for class discussion." They add 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. There are examples of security textbooks integrating case-related scenarios. For example Dhillon (2007) includes cases that describes a company's problem scenario as an introduction to each chapter, and then connects the case to theory at the end of each chapter by tasking students with answering case-related questions. The Information Systems Audit and Control Association (ISACA) also provides graduate-level teaching cases (ISACA, 2007; 2010) which emphasize corporate governance problems related to security management and the Control Objectives for Information Technology (COBIT) framework. Schembari applies cases to security law through student debate of legal case studies (Schembari, 2010). The case study presented in this paper, the Health First Case Study, is designed to give upper level undergraduate or graduate computer science, information systems, and information technology students an opportunity to plan security for a doctor's office, with the guidance of another useful resource, the Small Business Security Workbook.

The Health First Case Study (Lincke & Dorr, 2011) was developed to prepare students in developing security controls in a realistic setting. The case study along with the Small Business Information Security Workbook (Lincke, 2011b) may be used in courses for information systems, computer science, health IT, and management courses. The paper focuses on use of the case study to teach information systems related fraud concepts and prevention. The following sections include introductory concepts on fraud, an overview of the fraud prevention related Health First case studies, and notes on teaching the case study in both a face-to-face and online class setting.

INTRODUCTORY CONCEPTS

A discussion on fraud is an important first step before beginning the case studies. A set of lecture notes and presentation slides on fraud are provided to instructors using the Health First Case Study and Small Business Information Security Handbook (Lincke, 2011a). The lecture materials include a discussion on both internal and external fraud, and introduce the concept of controls for fraud prevention. This following section defines the high level overview of the topics included in the Fraud presentation and serves as background information for understanding the case studies.

Information systems fraud, often referred to as computer fraud or computer-related, may be divided into external and internal fraud, depending on whether the perpetrator is an employee or not.

External fraud includes social engineering techniques including scams that have been used in retail stores including check fraud (Abignale, 2001). The *Art of Deception* (Mitnick and Simon, 2002) describes several other social engineering schemes and defenses. For example, social engineers may use multiple phone calls: the first call obtains information or establishes a relationship, which is then used to obtain the real information or access in later calls. The fraudster attempts to sound like an insider. Defenses against social engineering may include 1) defining security classifications for data/resources; 2) ensuring employees verify identity before giving access to information or resources; and 3) training personnel for the policies and procedures, and in techniques of social engineering.

Internal or occupational fraud includes asset misappropriation, bribery and corruption, and financial statement fraud (Coenen, 2008). For a case to be successfully prosecuted, legal considerations of fraud include victim loss, personal material benefit, and intentional false representation. The key elements of fraud include: motivation, opportunity, and rationalization. Control techniques to discourage fraud include preventing or reducing the likelihood of these three key elements. For example, a strong defense against opportunity is segregation of duties.

CASE STUDY: THE HEALTH FIRST DOCTOR'S OFFICE

In the US, many doctor's offices or clinics are considered small businesses and must also adhere to federal laws governing privacy and security of patient information including the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its related security and privacy rules. The Health First Case Study was developed as a single case study in that the same organization is presented across the multiple challenges that are introduced. At the same time the specific challenges are presented as small case studies within the same organization (and document) and may be used separately or as a whole.

To help lead students through the case studies, a Small Business Information Security Workbook has also been developed that guides small businesses through the process of organizing a security program. The Small Business Information Security (SBIS) Workbook provides a procedure for building security plans for a generic small business. In combination the Health First Case Study along with the Small Business Information Security Workbook introduce students to a realistic organizational setting with a resource that may be used well beyond the end of the class. Each case study may be used as an active learning team exercise or as a single or paired homework assignment.

The following case studies were designed to address the goal of combating fraud:

1. Fraud: Combating Social Engineering
2. Developing a Code of Ethics
3. Update Requirements Document to Include Segregation of Duties
4. Designing Information Security
5. Planning for Incident Response
6. Organizing Personnel Security

The first case study introduces students to a social engineering attack via a hypothetical fraud case, and asks students to develop a procedure to combat social engineering. The remaining case studies help to reduce the probability of fraud, by defining control processes. Cases 2 and 3 help to control internal fraud, while cases 4-6 help to combat internal and external fraud. Cases 2 and 3 address two of the three key elements of fraud: opportunity, motivation, and rationalization. Case 2, Developing a Code of Ethics, addresses rationalization, while Case 3, Segregation of Duties, addresses opportunity. Case 4 and 5 address technical issues relating to internal and external fraud. Case 4, Designing Information Security, defines the technology and procedural controls that are required in normal operation, while Case 5, Planning for Incident Response, defines the procedural controls required after an attack has occurred. Once control procedures are defined via cases 1-5, then job descriptions should be updated and appropriate training is decided. This task is performed in 'Case 6 Organizing Personnel Security'. However, it is important to inform students that work in the cases is an iterative process, and it is not unusual to make changes in the previous case studies as later case studies are discussed and completed. Each case study is discussed in more detail below.

Case 1 - Fraud: Combating Social Engineering

This case study provides a hypothetical example, where a scoundrel uses his girlfriend to obtain medical information on his wife. The information is to be used against her in divorce proceedings, to obtain custody of the school-aged children during the week (and free his weekends). He hears that she may have cancer, and believes custody will go his way if he can somehow obtain the information. The man's girlfriend obtains the information via two calls: the first to learn of the appropriate doctor and appointment, and the second to obtain the health information. This hypothetical example is provided in conversation form, and clearly shows how the illegal medical information could be beneficial, and how simple it could be to acquire health information, by lying.

After reading the hypothetical social engineering case, students prepare a procedure to minimize the probability of a successful social engineering attack. This case study is an extension of the fraud lecture. To summarize the learning outcomes for this case study, students learn about social engineering, develop a procedure on how to combat it, and practice writing a professional procedure.

Case 2 - Developing a Code of Ethics

Case 2 introduces students to the Health First staff, and enables students to identify with both the business and IT technical perspectives. This case study can be used at the beginning of the semester, since it does not require deep security or technical knowledge.

The case study provides a conversation between Health First staff concerning various corporate ethical issues: employee conduct, employee use of organization resources, relationships with customers and suppliers, HIPAA privacy and confidentiality. A skeleton Code of Ethics is provided in the SBIS Workbook.

The outcome for the business is a Code of Ethics, which is meant to guide employee behavior. Learning outcomes for the students include an expanded view of the organization that includes both the business and IT view of the organization, discussion of expectations for ethical behavior in an organization, written policy-type documentation, and a Code of Ethics.

Case 3 - Update Requirements Document to Include Segregation of Duties

Case 3 investigates Segregation of Duties, which includes the responsibilities of origination, distribution, authorization, and verification. Segregation of Duties is traditionally a difficult idea to understand, so this case study discusses the role allocation in the Health First office. While the Fraud lecture introduces the segregation of duties concept, a Personnel Security lecture describes the topic in more detail. This case study does not use the Workbook, but instead modifies a Requirements Document. This has the advantage of showing technically-minded Computer Science and Information Systems students that their security knowledge can be used in designing requirements for software. IT students also need to understand their role in working with Requirements Documents.

The Segregation of Duties issue for Health First is that the Medical Administrator can create and bill a patient without any one overseeing their actions – or can choose not to, thereby pocketing any cash themselves. In addition, all Doctors have Medical Administrator permissions, because they need to be able to conduct business, even if the Medical Administrator is not present. Therefore, this case study considers solutions to this problem. Students modify the Requirements Document: 1) to implement a new state variable to ensure all transactions are processed accurately (serving as an automatic form of Verification), and 2) include a report that enables an Authorization role to validate transactions.

The outcome for the business is an IT software plan to cope with Segregation of Duties, which is a strong control against internal fraud. Learning outcomes include student application of a real-world Segregation of Duties problem, and integrating security into a professional Requirements Document.

Case 4 - Designing Information Security

Information Security addresses issues relating to internal and external fraud, including the technology and procedural controls that are required in normal operation. Students work with the Small Business Information Security Workbook to define an information security policy. A PowerPoint lecture on Information Security provides important concepts, with an example education-related case study solution for many of the Workbook case study tables.

The case study first directs students to consider Sensitivity and Criticality classifications for organizational data. Students then discuss how the data should be protected (e.g., for which data classifications should transmissions and data at rest be encrypted). Next, students define organizational roles and major data assets. Finally, they define which roles shall have access to which data: role-based access control considers who is allowed read/write/execute permissions to part or all of each computer form.

The outcome for the business is an information security plan within the Workbook. Learning outcomes include developing a data classification system and designing role-based access control.

Case 5 - Planning for Incident Response

Incident response deals with an internal or external fraud incident. There are six stages of incident response: Preparation, Identification, Containment, Analysis and Eradication, Recovery, and Lessons Learned (ISACA, 2009). Case 5, Planning for Incident Response, addresses Stage 1 Preparation, which prepares an organization for an incident (i.e., the remaining incident response stages). Presentation slides and lecture notes on incident response are provided to help present the six stages to students. The students work with the Small Business Security Workbook, which leads them through the security design process.

Case 5 leads students to define potential incidents as well as 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. The next step includes addressing 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.

The outcome for the business is 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.

Case 6 - Organizing Personnel Security

Organizing 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. Students work with the Small Business Information Security Workbook chapter on Personnel Security. Presentation slides and lecture notes on Personnel Security describes personnel security issues dealing with hiring/termination, different forms of security training, and segregation of duties. The lecture slides and notes also provide an example education-related solution to the Workbook case study tables for students to peruse while doing the case study.

Case 6 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. During the case study students review the Security Rule to allocate responsibility to the CSO and other employees to ensure adherence to HIPAA. Finally, the Workbook directs students to define the training and procedures that will enable everyone to complete their HIPAA responsibilities.

The outcome for the business is a coherent system of security, including allocation of security responsibilities, training, and documentation, when sufficient time is allocated to the assignment. As part of the case students evaluate security from the personnel perspective, consider security as a system, apply the HIPAA Security Rule, and review previous exercises.

NOTES ON TEACHING THE CASE STUDIES

The Health First Case Study may be taught as an active learning exercise in class, or as a homework assignment (perhaps for an Online course). The following sections discuss the experience of two different classes and course delivery methods. The case study materials are available since they were funded by NSF, including PowerPoint lecture slides and notes, the Health First Case Study, Small Business Information Security Workbook, and Small Business Requirements Document. There is also a Small Business Information Security Workbook Solution, which includes case study solutions.

In-Class Active Learning Exercise

PowerPoint lectures are given in the first half of a 3-hour face-to-face class, and the second half is the active learning exercise. The lectures have been enhanced to include appropriate example tables from the Small Business Security Workbook, for a University application. (The students will complete a Doctor’s office application.) The 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 instructor’s web page during the active-learning exercise.

During the active learning exercise, students move to a computer room where they can edit the Small Business Security Workbook (or Requirements Document) directly onto a computer. Students are grouped into 3-4 person teams, and each team is provided a computer. 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 each student with 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 subdivided 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 best way to start the case study is to have students select specific roles to play. To encourage this, we have students read the first part of each case study out loud, where each role is read by a different student. Most case studies have 4 roles, so there would normally be 4 readers. This has the advantage that students get to play the role of the IT person, versus a doctor or medical administrator. It also starts out the case study with students actively talking, and not silently reading (or being confused). If the case study is read out loud in front of the whole class, it enables the instructor the opportunity to start asking questions for class discussion, and getting initial ideas in play.

After the case study is being actively discussed per group, the instructor may see that some groups are too quiet or going in the wrong direction. It is possible to guide the students toward the right direction. 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 the case study web site.

For active learning, students are given credit for participating, and not on the work done. If students miss the active learning exercise, they can submit it as homework. Due to the 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!

For the Personnel Security case study, it is important that the HIPAA lecture has previously been given, and that the HIPAA lecture notes are also available to students. We print up copies of the HIPAA lecture, with sufficient copies for one for each group. The HIPAA lecture copies are retained for reference in the teaching lab, but distributed at the beginning of each lab, when this material is important.

Homework or Online Course

In an asynchronous online course the Health First Case Study cases are introduced through a lecture using the associated presentation slides and notes. Lecture notes and audio/video enhance the lecture for students. Students are given an electronic copy of the entire Small Business Information Security Workbook and the Health First Case Study document. If time permits, it may cause less confusion to provide only the section of the case study and workbook needed for the homework assignment.

Students were assigned the task of reading a specific section of the Small Business Information Security Workbook, which provides a model for the case study assignment. Then students are required to read the assigned Health First case study. For submission the students were required to use the SBIS Workbook example as a template and add any additional content by bolding, highlighting, or tracking the changes in the document. For example Directions provided for the Code of Ethics Case Study may be in the following format:

Example 1 – Developing a Code of Ethics Case:

> *The Small Business Information Security Workbook includes a recommended code of ethics for a small business (pages #-#). Use the example code of ethics and modify it to make it appropriate for Health First. The conversation on page #-# in the Health First Case Study provides suggested changes. Include your suggested Health First code of ethics in a Word (.doc/.docx) or Rich Text File (.rtf). Highlight by* ***bolding****; changing the color;* <u>*or*</u> *tracking your document changes to show the modifications you made to the document.*

Example 2 – Organizing Personnel Security

> *Background Reading:*
>
> - *Health First (Section 11. Personnel Security Planning; Pages # - #)*
> - *Small Business Security Workbook (Pages # - #)*

> *Using the information from the Health First reading assignment case study above and the supporting information in the Small Business Security Workbook, please complete the following which can be found in the small business security workbook:*
>
> 1. *Complete Table 4.6.1: Personnel Threats*
> 2. *Complete Table 4.6.2: Personnel Controls*
> 3. *Complete Table 4.6.3: Responsibility of Security to Roles*
> 4. *Complete Table 4.6.4: Requirements for Security Roles: Training & Documentation*
>
> *Submit all the completed tables in a single document (.doc, .docx, or .rtf).*

Each case submission was graded on a 10 or 20 point scale depending on the intensity of work for the case. The SBIS Workbook solution document was used as the standard for grading, and students were awarded points based on the quality, completeness, creativity, conciseness, and written mechanics of each task with the workbook solution document used as a guide. Students are not expected to submit an identical solution as the instructor solution document, and some students have difficulty being concise and assume quantity of information is a substitute for quality.

For continuous improvement and troubleshooting, a discussion board was attached to allow students to discuss the case and ask questions. In addition, an anonymous survey was available for students after each lesson to help identify areas of confusion and understand how well students felt they learned the concept.

RESULTS

Some data was collected during use of the case study in the in-class, face-to-face, version of the course. The course also included a community-based learning aspect, where students worked with a community partner to implement parts of the Workbook. 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 [community] partner”. However, there was also a consensus that ‘catching on’ in the first few case study labs was difficult.

It is true that later labs had higher approval ratings than earlier labs. Our first four case study 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” as opposed to a “disagree” answer). To fix this, we currently start the case study as a class (and not in 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.”

CONCLUSION

Fraud is an area that is not widely addressed in information security curricula. The problem of fraud is also not emphasized in the top certifications in information security management and IS auditing (i.e, the CISA, CISM, and CISSP). Computer science, information systems, and information technology students have the opportunity to experience security planning and management with the Health First Case Study, Small Business Information Security Workbook, and Small Business Requirements Document. The materials presented in this paper provide instructors with a rich resource for a course, including a set of case studies related to fraud.

The set of fraud-related Health First case study exercises demonstrates the issue of social engineering as a serious threat. The case studies also address preventive controls for three key elements of fraud: opportunity (segregation of duties), motivation (code of ethics), and rationalization (information security and personnel security policies). Finally, if an incident occurs, incident response is a detective/corrective control. Thus, the six case studies help educate students about a variety of fraud controls.

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.

REFERENCES

1. Abignale, F. (2001) The Art of the Steal, Broadway Books, New York.
2. Association of Certified Fraud Examiners. (2010) Report to the Nations, Last accessed on February 2, 2012, at http://www.acfe.com/rttn.aspx.
3. Coenen, T. L. (2008) Essentials of Corporate Fraud, T L Coenen, John Wiley & Sons, Hoboken, NJ.
4. Dhillon, G. (2007) Principles of Information Systems Security, John Wiley & Sons, USA.
5. ISACA (Information Systems Audit and Control Association). (2010) CISA® Review Manual 2011, 23-72.
6. ISACA (Information Systems Audit and Control Association). (2009) CISM Review Manual 2010.
7. ISACA (Information Systems Audit and Control Association). (2010) Information Security Using the CISM® Review Manual and BMIS™: Caselets, Rolling Meadows, IL.
8. ISACA (Information Systems Audit and Control Association). (2007) ITGI, IT Governance Using COBIT® and Val IT: Student Book, 2nd Ed., IT Governance Institute, Rolling Meadows, IL, 2007.
9. Lincke, S. J. (2011) Security Planning Resources. Last Accessed on February 6, 2012, at http://www.cs.uwp.edu/staff/lincke/infosec/
10. Lincke, S. J. (2011) Small Business Information Security Workbook. Last Accessed on February 1, 2012, at http://www.cs.uwp.edu/staff/lincke/infosec/notes/SecurityWorkBook.doc
11. Lincke, S. J., and Dorr, Tim, (2011) Health First Case Study. Last Accessed on February 1, 2012, at http://www.cs.uwp.edu/staff/lincke/infosec/notes/MedCaseStudy.doc
12. Mitnick, K., and Simon, W. (2002) The Art of Deception, Wiley & Sons, Indianapolis, IN.
13. Panko, Raymond. (2010) Corporate Computer and Network Security, 2nd Edition, Upper Saddle River, NJ.
14. Schembari, N.P. (2010) An Active Learning Approach for Coursework in Information Assurance Ethics and Law, *Proceedings of the 14th Colloquium for Information Systems Security Education (CISSE)*, 1-8.
15. Wei, H. Xin, C. and Ying, H. (2010) Non-computer Professional IT Education in the MBA Model, *Proceedings of the 5th International Conf. on Computer Science & Education*, IEEE, 612-614.