Teaching Security Management with Case Studies: Experiences and Evaluation

Xiaohong Yuan[1], Keyu Jiang[2], Sahana Murthy[1], Jonathan Jones[1], Huiming Yu[1]
[1]Department of Computer Science
North Carolina A&T State University
Greensboro, NC 27411, U.S.A.
Phone: (336)3347245 Fax:(336)3347244
Email: xhyuan@ncat.edu

[2]Dept. of Informatics
Fort Hays State University
Hays, KS 67601-4099 U.S.A
Phone: (785)6284684
Kjiang@fhsu.edu

ABSTRACT

Teaching with case studies is an effective method that actively engages students. This paper describes two case studies we developed and our experiences teaching security management with these two case studies. The case studies were used to teach risk management and incident response planning. Each case study includes the learning objectives, one/more case scenarios and a series of case discussion questions. The student feedback on these case studies was very positive. Our future work will include refining the developed case studies, continuing to evaluate their effectiveness, developing more case studies, and exploring different ways of teaching case studies.

Keywords: security management, information security education, case study, risk management, incident response planning

1. INTRODUCTION

Security management is an important topic taught in an information security program. This paper introduces our experiences of teaching security management using case studies. Teaching with case studies helps students to learn actively and provides opportunities for them to develop their communication, teamwork, and problem solving skills. It also increases students' enjoyment in learning [1]. Case discussions can bring life to the classroom, arouse student interests, and apply their learning to the real world situations. Case study method is especially suitable for teaching security management concepts due to the richness of real life experiences in this area.

In this paper, two case studies for teaching security management are described. They are: (1) the hypothetical computer system risk management case study; (2) the incident response planning case study. These case studies were developed and taught in the "Foundations of Information Systems Security" course at Fort Hays State University. The case studies provide education on both the awareness level and the performance level on contingency planning/disaster recovery based on National Training Standard For Information Systems (NSTISSI No.4011)[2]. Each case study includes the learning objectives, one/more case scenarios and a series of case discussion questions.

We used Bloom's taxonomy to guide our design of the learning objectives and discussion questions of the case studies. Bloom's taxonomy defines six levels of cognitive skills and capabilities. They are briefly described below [3].

Level 1: Knowledge. Recall data or information.

Level 2: Comprehension. Grasp the meaning of information materials.

Level 3: Application. Apply a concept in a new situation to solve problems.

Level 4: Analysis. Breakdown informational materials into components to understand the organizational structure.

Level 5: Synthesis. Create a new meaning or structure by applying prior knowledge and skills.

Level 6: Evaluation. Judge the value of informational materials.

It is important to set our teaching goals for students to demonstrate that they've learned skills and tasks from each cognitive category, but with an emphasis on the higher order cognitive tasks. Therefore the learning objectives and case discussion questions are designed such that they map to all the six cognitive levels of Bloom's taxonomy while stressing higher level skills.

In the following sections each of the case studies is described. The learning objectives, case description, student assignment, teaching methods, evaluation of the case study are discussed for each case study.

2. RISK MANAGEMENT CASE STUDY

Risk management is the process of identifying vulnerabilities in an organization's information systems and taking measures to ensure the confidentiality, integrity, and availability of the information system components. It includes two major steps: risk identification and risk control. In risk identification, the security profile of an organization and the risks it faces are examined and documented. In risk control, measures are taken to reduce the risk to an organization's information systems [4].

This case study illustrates the risk management process of a hypothetical government agency. The learning objectives of this case study are:

1. Identify the threats facing the assets of an organization.
2. Determine the probability of threats, and their potential impact.
3. Determine risk rating/scale.

4. Identify current control measures.
5. Identify vulnerabilities of computer systems.
6. Recommend risk mitigation strategies for controlling risks.
7. Choose risk mitigation methods.
8. Evaluate the management decision on risk mitigation strategies based on cost benefit analysis.

2.1 Case Description

The hypothetical computer system risk management case study is based on "Assessing and mitigating the risks to a hypothetical computer system" (AMRHCS) case from NIST Special Publication 800-12 [5]. In the AMRHCS case, the Hypothetical Government Agency (HGA) initiated a comprehensive risk analysis process to assess its security program. HGA's assets and computer systems, threats to HGA's assets, HGA's current security measures, vulnerabilities found by the risk assessment team, the recommendation for mitigating the identified vulnerabilities, as well as the management's final decisions are described in detail in the AMRHCS case.

2.2 Case Discussion Questions

There are five categories of threats to HGA's assets: payroll fraud, payroll errors, interruption of operations, disclosure/brokerage of information, and network related threats. The case discussion questions are divided into five parts according to the five categories of threats. For each threat category, a series of questions are asked. For example, the questions in Table 1 correspond to payroll fraud threat. Discussion questions for other threat categories are similar to those in Table 1. Table 1 also shows the mapping of the questions to Bloom's Taxonomy. The students were given reference [6] for answering the discussion questions.

3. INCIDENT RESPONSE CASE STUDY

Incident response planning involves identifying, classifying and responding to an incident. According to the NIST special publication 800-61[7], incident response life cycle includes four phases: (1) preparation and planning, (2) detection and analysis, (3) containment, eradication, recovery, and (4) post incident activity.

In the preparation and planning phase, an incident response team should be formed. The team is composed of members from various functional roles in the organization. In the detection and analysis phase, potential incident information is monitored and gathered. Incidents are identified and classified into different categories according to their severity. Containment phase includes activities to minimize and isolate the damage incurred. After an incident is contained, eradication may be necessary to successfully eliminate the components of the incident. The recovery phase restores the operation of the compromised systems to normal business mode. Post incident activity usually includes a lessons-learned meeting in which the incident is reviewed, and the weakness of the incident response plan is identified. The incident response plan is then updated and the incident is documented in detail.

NIST special publication 800-61[7] categorizes four different types of incidents: denial of service, malicious code, unauthorized access and inappropriate usage. For each of the categories, NIST provides guidelines for how to prepare for, prevent, detect and analyze, contain, eradicate, and recover from the incidents.

The case study we designed for teaching incident response planning has the following learning objectives:

1. Identify an incident.
2. Classify an incident according to its severity.
3. Identify the roles and responsibilities in an incident response team.
4. Identify the steps an organization should take to contain and recover from an incident.
5. Recommend measures to prevent similar incidents from occurring in the future.
6. Recommend actions to improve the detection of similar events.

3.1 Case Description

This case study includes a realistic incident response plan "XYZ University Computer Security Incident Response Plan" and two real-life scenarios. For each scenario a series of questions were designed that correspond to the learning objectives of this case study. The students were to use NIST special publication 800-61[7] and book [1] as references.

The XYZ University Computer Security Incident Response Plan defines the roles and responsibilities for the Chief Information Officer, Computer Incident Response Team, Information Security Officer and the supporting groups. It classifies incidents into four severity levels, namely, low, medium, high, and critical levels. For each severity level of incidents, CIRP describes the roles involved and their responsibilities for handling the incident. The CIRP also describes the post incident activity and provides an incident review report template.

The two scenarios given to the students are based on NIST Special publication 800-61 [7] Appendix B "Incident Handling Scenarios". These two scenarios illustrate malicious code attack and inappropriate usage attack.

Table 1. Discussion questions on payroll fraud threat

Risk Management Case Discussion Questions	Cognitive Levels
1. What are the different types of payroll fraud threats?	Level 2 - Comprehension
2. What is the probability of payroll fraud threats (in terms of high, medium, low)? What is the potential impact of payroll fraud threats (in terms of high, medium, low)? Explain. Refer to [6].	Level 4 – Analysis
3. According to the Risk-Level Matrix in [6], determine the risk scale of payroll fraud threats.	Level 3 – Application
4. What are the control measures currently in use to protect against payroll fraud?	Level 2 – Comprehension
5. What are the vulnerabilities related to payroll fraud found by the risk assessment team?	Level 2 – Comprehension
6. What's the recommendation by the risk assessment team?	Level 2 – Comprehension
7. What are the final decisions made by HGA management? Justify their decisions based on cost benefit analysis.	Level 4 – Analysis Level 6 - Evaluation

Scenario 1:

On Thursday morning, John, an XYZ university employee, noticed a warning message on his computer saying that the system has been attacked by a worm Win32.VB. Even though the antivirus software was present in the system, the software failed to detect the new worm because it was not updated to the latest version. When John tried to open his e-mail, he experienced a slow internet connection. He noticed there were some unusual file names in the disk. John immediately informed his friend Bob, who was also an XYZ employee, of the problem. Bob checked his computer in his office and experienced the same problem as John. John and Bob checked several computers in the laboratories, and found that Win32.VB worm had infected many other computers in the laboratory. They contacted the system administrator of the XYZ University. The system administrator checked the computers in the laboratory and reported the incident to the incident response team. The system administrator also checked the computers in other laboratories. As a result of the worm attack the activities in the XYZ University laboratory were suspended for a day, which caused a great inconvenience.

Scenario 2:

On a Monday morning, the XYZ University's legal department received a phone call from the Federal Bureau of Investigation (FBI) regarding some suspicious activity originating from the XYZ University's network. Later that day, an FBI agent met with the members of management and the legal department to discuss the activity. The FBI has been investigating activity involving online purchases made with several stolen credit card numbers. More than 30 of the transactions during the past week had been traced to one of the XYZ University's IP addresses. The FBI agent asked for the organization's assistance, and in turn, the managers asked for the incident response team's assistance in acquiring evidences. It is vitally important that this matter be kept confidential.

3.2 Case Discussion Questions

The case discussion questions for the incident response planning case study and their mapping to Bloom's taxonomy are listed in Table 2.

4. EVALUATION

The two case studies were used in the "Foundations of Information Systems Security" course at Fort Hays State University in the Fall 2009 semester. Thirty one students were enrolled in the course. The following two sections describe our experiences teaching these two case studies and the evaluations of these two case studies respectively.

4.1 Evaluation of Risk Management Case Study

After introducing to the students the basic concepts of risk management in the lecture, the students were given the risk management case study as a group project. Each group includes three students. The students were given the article "Assessing and mitigating the risks to a hypothetical computer system" [5] and NIST special publication 800-30 [6] as references for the project. Since the discussion questions of this case study is divided into five parts according to the five different types of threats, each group will answer one part of the discussion questions, and the whole class will cover all the five parts. The students are to submit a written answer to the discussion questions, and give a class presentation. The students were given two weeks to finish the project.

Before they started with the project, the students were asked to fill out a pre-survey. The pre-survey asks the students to rate their level of knowledge or skills on the eight learning objectives of this case study (see Section 2). The following scale is used to rate their level of knowledge: 1 (very low), 2 (medium low), 3 (medium), 4 (medium high), and 5 (high).

After the students completed the project, the students were asked to complete a post-survey. The post-survey has three parts. The first part asks the students to rate their level of knowledge or skills on the same learning objectives of this case study. The second part gives a series of statements, and asks the students to choose how much they agree with the statement by selecting (a) Strongly agree, (b) Agree, (c) Neither agree or disagree, (d) Disagree, and (e) Strongly disagree. The statements included in the post-survey are listed in Table 3. The third part asks the students to answer what they liked best about the project, what they liked least about the project, and what could be improved in the project.

Paired t-test was run on the students' ranking of their knowledge and skills on the learning objectives on the pre-survey and post-survey. The t-test results (see Table 4) show that the post-survey results are significantly higher than the pre-survey results. This shows that the students believed that they improved their knowledge/skill after the project on all the eight learning objectives.

Figure 1 shows the results of how much the students agree with statements (a) to (f) shown in Table 3. On average 85% of the students agree or strongly agree with the statements.

.Table 2. Discussion questions for incident response case study

Incident Response Case Discussion Questions	Cognitive Levels
1. Would the organization consider this activity as an incident? Justify your answer	Level 3 - Application
2. What's the severity level of the above mentioned incident?	Level 3 - Application
3. Who or what groups will be involved in the situation?	Level 3 - Application
4. Suggest measures to contain and recover from the incident.	Level 5 – Synthesis
5. Suggest measures to prevent similar incidents from occurring in the future.	Level 5 - Synthesis
6. Suggest actions to improve the detection of similar events	Level 5 - Synthesis

Table 3 The statements on post-survey

(a) This project is practical and will help you to apply what you learned to a job you may have in the future.
(b) You enjoyed working on the project.
(c) This project increased your understanding of risk management.
(d) This project stimulated your interest in learning risk management and information security.
(e) This project combined classroom and real-life experiences.
(f) This project helped with your motivation in learning risk management and information security.

Table 4. T-test results of students' ranking of their knowledge/skills on risk management

	Obj. 1	Obj. 2	Obj. 3	Obj. 4	Obj. 5	Obj. 6	Obj. 7	Obj. 8
pre-survey mean	3	2.73	2.36	2.73	3.05	2.68	2.36	2.45
pre-survey variance	0.57	0.68	0.81	1.16	1.38	1.08	0.72	0.93
Post-survey mean	3.64	3.45	3.45	3.41	3.59	3.41	3.27	3.36
post-survey variance	0.43	0.64	0.83	0.73	1.11	0.63	0.68	1.10
degree of freedom	21	21	21	21	21	21	21	21
observations	22	22	22	22	22	22	22	22
two-tail *p*-value	0.0005	8.43E-05	0.0002	0.0042	0.0023	0.0046	0.0006	0.0030

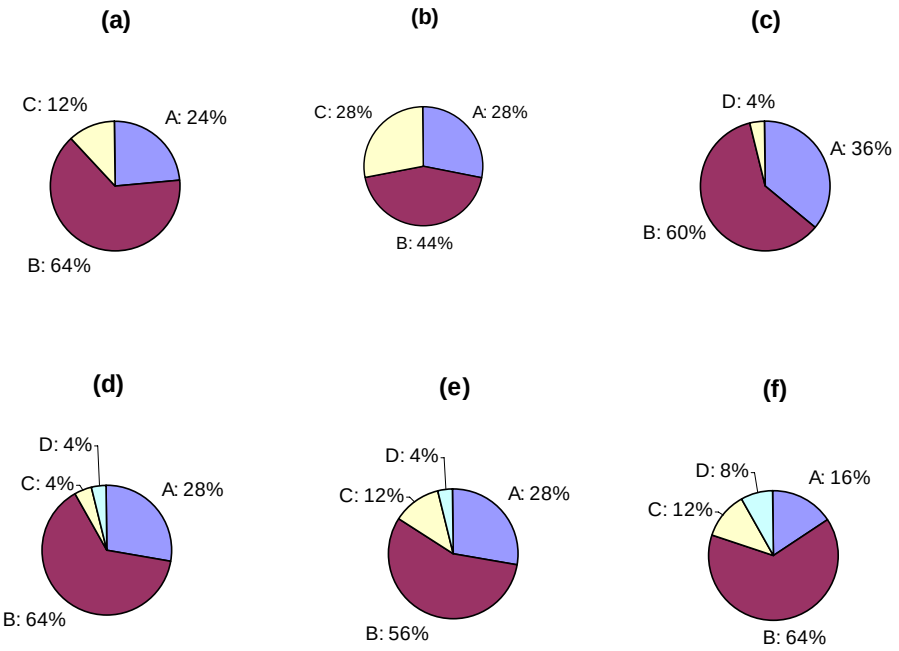

Figure 1. The results of how much the students agree with statements (a) to (f)

The students' comments on what they liked about the project include:

- The case study was a very realistic scenario that any information security professional may encounter
- The project gave a chance to apply classroom lessons to a potential real life situation.
- This project goes through the whole process of risk management rather than just some aspects and parts,. The project helped students to see the bigger picture rather than just the pieces.
- This project allows the students to work in groups and includes group presentations.
- The project illustrated that there are several other aspects of a 'process' (such as payroll), other than just putting the data into the computer and extracting it in the future.
- This project helps students to learn the importance of information security.
- This project helps students to learn much knowledge about information security.
- The discussion questions are critical for students in the future as professionals.
- The reading reference is very helpful for completing this project.
- Many of the considerations appeared to come from a real-life basis, although it was about a fictitious company. … It demonstrates how a solution about one particular department's problem could be applied at a later time to other departments to holistically improve layers of security across a company. It also demonstrates the overlapping issues. For example, very similar adverse results can be experienced by a company due to either fraud or a data entry error and both adverse results carry a similar amount of risk and priority to fix.

Some suggestions on improving this case study include:

- Update the case with a risk assessment that would reflect more current trends.
- Provide clarification on whether the presentation should convey what we learned from doing the project or if it should be based on our findings specific to HGA.
- Allow the students to choose which part of the discussion questions they should work on.
- Introduce to the students how to conduct case study before they take the project.
- Add more references to encourage the students to look for information other than in the case study and may be introduce ideas from CISSP to the case study.
- Make it a real life situation with a local company and make it more touch and feel for on-campus students.
- Organize an in-class discussion of this project. This provides an opportunity for inter-team

communications since each team just took one part of the project.

- Make the questions more specific.
- Have two teams working on two different areas of the Common Body of Knowledge (CBK) together.
- Provide a specific rubric for how the students will be graded.
- Include video clips in the references.
- Use anonymous survey.

Overall student feedback on the risk management case study is very positive.

4.2 Evaluation of Incident Response Case Study

After introducing to the students the basic concepts of incident response planning in the lecture, the students were given the incident response planning case study as an individual project. The students were given "XYZ University Computer Security Incident Response Plan" and the two scenarios. For each scenario, the students were asked to answer the discussion questions listed in section 3 and then give a presentation based on the discussion questions. The students were given two weeks to finish the project.

The students were asked to fill out a pre-survey before the project and a post-survey after the project. The pre-survey asks the students to rate their level of knowledge or skills on the six learning objectives of this case study (see Section 3) using the same scale as in the risk management case study. The post-survey includes the students' rating of their level of knowledge or skills on the same learning objectives of the incident response case study, students' level of agreement with the statements similar to those listed in Table 3, and what they liked best and least about the project, and what could be improved in the project.

Paired t-tests were run on the students' ranking of their knowledge and skills on the learning objectives on the pre-survey and post-survey. The t-test results (see Table 5) show that post-survey results are significantly higher than pre-survey results. The students believed that they improved their knowledge/skill after the project on all the six learning objectives of the case study.

Figure 2 shows the results of how much the students agree with statements (a) to (f) shown in Table 3. On average 78% of the students agree or strongly agree with the statements.

Table 5. T-test results of students' ranking of their knowledge/skills on incident response planning

	Obj. 1	Obj. 2	Obj. 3	Obj. 4	Obj. 5	Obj. 6
pre-survey mean	2.94	2.69	2.56	2.69	2.63	2.63
pre-survey variance	0.73	0.76	1.46	1.03	0.92	1.45
post-survey mean	3.94	3.81	3.94	3.88	4.06	3.81
post-survey variance	0.46	0.30	0.60	0.52	1.00	0.96
degree of freedom	15	15	15	15	15	15
observations	16	16	16	16	16	16
two-tail *p*-value	0.0004	0.0003	7.84E-05	0.0002	2.59E-05	0.0004

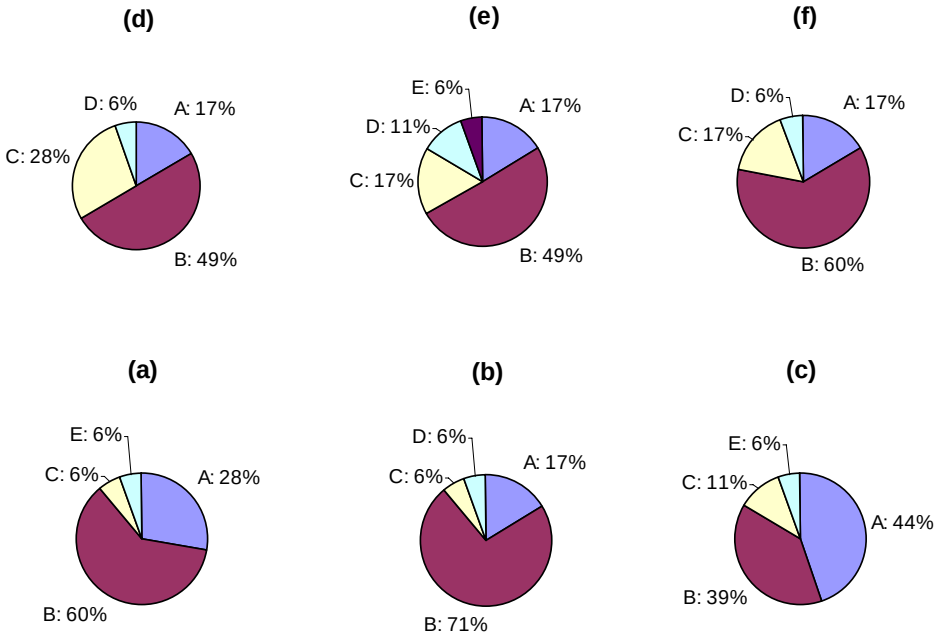

Figure 2. The results of how much the students agree with statements (a) to (f)

The students' comments on what they liked about the project include:

- This project increased students' understanding of incident response planning.

- It teaches many prevention measures for similar incidents.
- Students worked with some interesting scenarios and detailed information was provided to complete the case study.
- It is the real-world application of incident response concepts. It uses examples from real life to teach information from books.
- Students learn how to face problems, and how to make an incident response plan.
- This project is very important and is beneficial for work in the future.
- This case provides a new channel to understand Information Technology.
- NIST document was provided for students to refer to, which is real material that is used in the field.
- There was room given to students so that students could try to come up with what they would do about the situations rather than giving a response from something that was already determined. The students were challenged to get creative, do research.

Some suggestions on improving this case study include:

- Provide more details for each scenario
- Allow the students to work in a group

Overall student feedback on the incident response planning case study was very positive. Though some students would like the case scenarios to be more specific, others appreciate that it had room for students to get creative and do research. It is important to be balanced and provide appropriate amount of details when designing a case study.

5. CONCLUSION

This paper describes our experiences teaching security management using the approach of case studies. Two case studies were developed for teaching risk management and incident response planning. They were taught in the "Foundations of Information Systems Security" course in the Fall 2009 semester. Each case study includes the learning objectives, the case scenarios with supporting documents, and the case discussion questions. The case discussion questions were mapped to all the levels of Bloom's taxonomy.

Each case study was evaluated by a pre-survey and post-survey on the students' ranking of their knowledge and skills on the learning objectives. The t-test results show that the students believed that they improved their knowledge/skill after the project on all the learning objectives of the case studies. Most students agree that the case studies helped them to relate classroom learning to real-life experiences, and increased their interest and motivation in learning information security. Some students suggested adding more details to the case descriptions, or making the discussion questions more specific. Overall, the student feedback is very positive.

In the future, we plan to improve these case studies according to student feedback and continue assessing their effectiveness in teaching. We will explore various approaches of teaching case studies and develop more case studies in the area of security management as well as in other areas of information assurance.

6. REFERENCES

[1] Penn State University Teaching and Learning Technology, Using cases in teaching, available at: http://tlt.its.psu.edu/suggestions/cases/index.html

[2]NSTISS, National Training Standard for Information Systems Security (INFOSEC) Professionals, 1994, www.cnss.gov/Assets/pdf/nstissi_4011.pdf.

[3]Assessing Student Learning at the End of the Semester: Bloom's Taxonomy, available at: http://web.princeton.edu/sites/mcgraw/Scholar_as_Teacher_assessing_student_learning_at_the_end_of_the_semester_bloom's_taxonomy_28.html

[4] Whitman, M.E. and Mattford, H.J. *Principles of Information Security 3rd Edition*, Thomson Course Technology, 2005

[5] National Institute of Standards Technology Standard, "Chapter 20 Assessing and Mitigating the risks to a hypothetical computer system", *An Introduction to Computer Security: The NIST Handbook*, http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf, pp. 243-267.

[6] National Institute of Standards Technology Standard, *Risk Management Guide for Information Technology Systems*, NIST special publication 800-30. Available at: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

[7] National Institute of Standards and technology. *Computer Security Incident Handling Guide, The NIST Handbook SP 800-61*, available at: http://www.nist.org/nist_plugins/content/content.php?content.42

ACKNOWLEDGEMENT

This work was partially supported by National Science Foundation under the award number DUE – 0737304 and by Department of Education under grant P120A090049.