# Case Studies for Teaching Physical Security and Security Policy

Xiaohong Yuan
North Carolina A&T State University
1601 East Market St.
Greensboro, NC 27411
(336)3347245
xhyuan@ncat.edu

Sahana Murthy
Credit Suisse
1416 Spring Garden Dr.
Morrisville, NC 27560
(336)4146566
Sahana.vm@gmail.com

Jinsheng Xu, Huiming Yu
North Carolina A&T State University
1601 East Market St.
Greensboro, NC 27411
(336)3347245
Cshmyu@ & jxu@ncat.edu

## ABSTRACT

Teaching with case studies is an important method that engages students in active learning. This paper describes two case studies we developed and our experiences teaching information security with these two case studies. The case studies were used to teach physical security and security policy. Each case study includes the learning objectives, case description and a series of case discussion questions. The case discussion questions were mapped to Bloom's taxonomy and Fink's taxonomy. Our teaching methods and student feedback are described. 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.

## Categories and Subject Descriptors

K.3.2 [**Computers and Education**]: Computer and Information Science Education – *information systems education.* K.6.5 [**Management of Computing and Information Systems**]: Security and Protection – *physical security.*

## General Terms

Management, security.

## Keywords

Information security education, case study, physical security, security policy.

## 1. INTRODUCTION

Teaching with case studies is an important method that engages students in active learning. It provides opportunities for students to develop their communication, teamwork and problem solving skills. It can bring life to the classroom, arouse student interests, increase student enjoyment in learning, and allow students to apply their learning to the real world situations [1]. Case study method is suitable for teaching information assurance due to the richness of real life experiences in this field.

This paper describes two case studies we have developed for teaching physical security and security policy. Each case study includes the learning objectives, case description, and a series of case discussion questions. Our experiences using these case studies are also discussed.

Bloom's cognitive taxonomy [2] defines six levels of learning that are arranged in a hierarchical sequence. They are:

**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 material.

Bloom's taxonomy has been used as a framework for formulating course objectives and as a basis for evaluating student learning. However, there has been a need for new kinds of significant learning that do not emerge easily from Bloom's Taxonomy. Examples of such learning include: learning how to learn, leadership and interpersonal skills, ethics, the ability to adapt to change, etc. Based on this need, Fink constructed a taxonomy that consists of six kinds of significant learning [3]:

**Foundational knowledge**: understanding and remembering information and ideas.

**Application**: Learning how to engage in various kinds of action including thinking, developing certain skills or learning how to manage complex projects.

**Integration:** Seeing and understanding the connections between different things.

**Human Dimensions:** Learning something important about their own self and/or about others.

**Caring:** Changing the degree to which students care about something, for example, new feelings, interests, and/or values.

**Learning how to learn:** Learning something about the process of learning itself, for example, learning how to be a

InfoSecCD'10, October 1-2, 2010, Kennesaw, GA, USA.
Copyright © 2010 ACM 978-1-60558-661-8/10/10…$10.00.

better student, how to engage in a particular kind of inquiry or how to become self-directing learners.

It is important to set our teaching goals for students to demonstrate that they've learned skills and tasks from each cognitive category of Bloom's taxonomy, 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. We've also mapped the case discussion questions to the Fink's taxonomy with the goal of achieving significant learning.

In the following sections each of the case studies is described. The learning objectives, case description, case discussion questions and their mapping to the Bloom's and Fink' taxonomies, and our teaching experiences are discussed for each case study.

# 2. PHYSICAL SECURITY CASE STUDY

Physical security includes the physical protection of people, hardware, and the supporting system elements and resources. It includes protection from fire, natural disasters, terrorism, etc. The control of physical access to the assets of an organization is a very important aspect of physical security. Some of the physical control methods include: identification cards, badges, electronic monitoring, alarm systems, etc. [4, 5] The learning objectives of this case study include:

1. List security technologies used for physical access control.
2. Identify physical security issues in a large corporate with many facilities all over the world.
3. Examine how the corporate solves its physical security problems.
4. Discuss the advantages of a solution to physical security over its alternatives.

## 2.1 Case Description

This case study is based on the article "How Cisco IT Controls Building Security over the Enterprise WAN" [6], which describes why and how Cisco Systems transitioned from standalone access control systems to an IP networked system to help secure its business facilities. This article discusses the history of physical-security issues in Cisco, the challenges that Cisco faced, and the solution Cisco has developed to overcome the challenges. Based on this article, we developed a series of discussion questions. These questions are listed in the next section.

## 2.2 Case Discussion Questions

The case discussion questions are mapped to Bloom's Taxonomy and Fink's Taxonomy. Table 1 and Table 2 list the case discussion questions and their mappings to Bloom's and Fink's taxonomies respectively.

## 2.3 Teaching Experience

This case study was used in an undergraduate course "Fundamentals of Information Assurance" in the Spring 2010 semester at this university. After introducing the basic concepts of physical security to the students in the lecture, the students were given the Cisco case study as a group project. Each group includes two to three students. After one week, the students submit a written answer and gave a class presentation. The students were given a survey after the project was completed. The survey result is summarized in Table 3. The survey result shows that student feedback is very positive

# 3. SECURITY POLICY CASE STUDY

Information security policy is the foundation of a quality security program. According to NIST Special Publications 800-14 [7], there are three different types of policies: (1) enterprise information security policies; (2) issue-specific security policies; (3) system-specific security policies. Enterprise information security policy guides the development, implementation, and management of the security program; Issue-specific policies instruct employees on the proper use of various technologies and processes; System-specific policies are standards or procedures to configure or maintain a system. This case study focuses on enterprise information security policy and issue-specific policy. The learning objectives for the security policy case study are:

1. Explain the importance of security policies to an organization.
2. Explain the aspects that should be included in a security policy.
3. Create an issue specific policy.
4. Critique a security plan and update the plan.

**Table 1. Mapping of Cisco case discussion questions to Bloom's Taxonomy**

| Physical Security Case Discussion Questions | Cognitive Level |
|---|---|
| 1. Why did Cisco Systems transit from standalone physical access control systems to an IP networked systems? | Level 4 – Analysis |
| 2. What challenges did Cisco Systems face in order to solve the physical security problems? | Level 1 – Knowledge<br>Level 2 – Comprehension |
| 3. How did the new architecture solve the physical access control problem? Explain. | Level 2 – Comprehension |
| 4. How did Cisco Systems solve the physical security problems? | Level 2 – Comprehension<br>Level 4 – Analysis |
| 5. What security technologies did Cisco deploy to control building security? | Level 2 – Comprehension |
| 6. Even though the employees in the Cisco Systems have doubled the STS team remains the same, why? | Level 4 – Analysis |

## 3.1 Case Description

In this case study students are given two sample security policies: (1) North Carolina Agricultural and Technical State University (NC A&T SU) security policy [8]; (2) Griffith University security policy [9]. The Students are to read the policies and answer the case discussion questions. Some of the discussion questions ask the students to critique and improve the policies. The students are asked to refer to the sample policies provided by SANS organization as references [10, 11, 12].

## 3.2 Case Discussion Questions

Table 4 and Table 5 map the case discussion questions to Bloom's and Fink's taxonomies respectively

**Table 2. Mapping of Cisco case discussion questions to Fink's Taxonomy**

| Fink's Taxonomy | Mapping |
|---|---|
| 1. Foundational knowledge | Security technologies for physical access control, problems with standalone access control systems in large corporation, advantages of centralized IP based architecture for physical security. |
| 2. Application | Thinking: critical thinking and practical thinking<br>Skills: analytical skills |
| 3. Integration | Network access control, security policies, global system integration, centralized control, scalability, cost benefit analysis in the security technologies, information security, risk management |
| 4. Human dimensions | N/A |
| 5. Caring | Appreciate the complexity of corporation and physical access control issues, the challenges in implementing policies and global integration models for large corporations, the importance of scalable solutions and solutions that reduce the cost in the long run. |
| 6. Learning how to learn | Learn from real world experiences |

**Table 3. Physical security case study student survey (number of students = 10)**

| Question | Response |
|---|---|
| This project is practical and will help you to apply what you learned to a job you may have in the future | 40% strongly agree<br>50% agree<br>10% neither agree or disagree |
| This project combined classroom and real-life experiences | 40% strongly agree<br>40% agree<br>20% neither agree or disagree |
| You enjoyed working on the project. | 40% strongly agree<br>40% agree<br>10% neither agree or disagree<br>10% disagree |
| This project increased your understanding of physical security | 60% strongly agree<br>40% agree |
| This project stimulated your interest in learning information security | 30% strongly agree<br>60% agree<br>10% disagree |
| This project helped with your motivation in learning information security. | 40% strongly agree<br>50% agree<br>10% disagree |
| The level of difficulty of this project is appropriate | 40% strongly agree<br>50% agree<br>10% neither agree or disagree |
| The project helped you to develop problem solving and critical thinking skills, and ability to think independently | 50% strongly agree<br>40% agree<br>10% neither agree or disagree |

## 3.3 Teaching Experience

This case study was also used in the undergraduate course “Fundamentals of Information Assurance” in the Spring 2010 semester at this university. After introducing the basic concepts of security policy to the students in the lecture, this case study was given to the students as a group project. Each group includes two to three students. After one week, the students submit a written answer and gave a class presentation.

To evaluate student learning, we gave the students a pre-survey before they started with the project. The pre-survey asks the students to rate their level of knowledge or skills on the four learning objectives of this case study. 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 third part asks the students the following questions: (1) what was the most important thing they learned; (2) what problem did they encounter; (3)what changes could be made to enhance their learning.

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 6) show the post-survey results are significantly higher than pre-test results ($p<0.05$). This shows that the students believed that they improved their knowledge/skill after the project on all the four learning objectives. Table 7 summarizes the student survey results. Table 7 shows student feedback was very positive. Some students felt that this was a very appropriate assignment for their level of knowledge of security policy. Some students would like to have more guidance on how to critique a policy.

**Table 4. Mapping of security policy case discussion questions to Bloom’s taxonomy**

| Security Policy Case Discussion Questions | Cognitive Level |
|---|---|
| 1. What is a security policy and why does an organization need a security policy? | Level 1 – Knowledge |
| 2. Come up with an example of your own, which would be caused by missing security policies. | Level 3 – Application |
| 3. What are the basic things that need to be explained to every employee about a security policy? At what point in their employment? Why? | Level 3 – Application |
| 4. Say you have an e-mail server that processes sensitive emails from important people. what kind of things should be put into the security policy for the email server? | Level 5 – Synthesis |
| 5. Read the NC A&T SU security plan and critique the plan. | Level 6 – Evaluation |
| 6. Read the Griffith university plan and critique the plan. | Level 5 – Synthesis |
| 7. Update theNC A&T SU security plan. | Level 5 – Synthesis |

**Table 5. Mapping of security policy case discussion questions to Fink’s taxonomy**

| Fink’s Taxonomy | Mapping |
|---|---|
| 1. Foundational knowledge | The importance of security policy, the components of security plan |
| 2. Application | Creative thinking, critical thinking and practical thinking; synthesis and evaluation skills |
| 3. Integration | Risk management, contingency planning, physical security, network security, information technology, business administration, law, ethics |
| 4. Human dimensions | N/A |
| 5. Caring | Appreciate the importance of having policies and abiding by the policies |
| 6. Learning how to learn | Construct knowledge based on examples, evaluate policy based on standard templates |

**Table 6. t-test results of students' ranking of their knowledge/skills on security policy**

| | Obj. 1 | Obj. 2 | Obj. 3 | Obj. 4 |
|---|---|---|---|---|
| pre-survey mean | 2.56 | 1.89 | 1.56 | 1.67 |
| pre-survey variance | 1.03 | 0.86 | 0.53 | 0.5 |
| Post-survey mean | 4.56 | 4.22 | 3.89 | 4 |
| post-survey variance | 0.28 | 0.69 | 1.36 | 0.75 |
| degree of freedom | 8 | 8 | 8 | 8 |
| Observations | 9 | 9 | 9 | 9 |
| two-tail *p*-value | 0.0001 | 0.0004 | 0.0011 | 0.0004 |

**Table 7. Security policy case study student survey results (number of students = 11)**

| Question | Response |
|---|---|
| This project is practical and will help you to apply what you learned to a job you may have in the future | 55% strongly agree<br>45% agree |
| This project combined classroom and real-life experiences | 45% strongly agree<br>55% agree |
| You enjoyed working on the project. | 18% strongly agree<br>64% agree<br>18% neither agree or disagree |
| This project increased your understanding of physical security | 64% strongly agree<br>36% agree |
| This project stimulated your interest in learning information security | 9% strongly agree<br>82% agree<br>9% disagree |
| This project helped with your motivation in learning information security. | 27% strongly agree<br>64% agree<br>9% disagree |
| The level of difficulty of this project is appropriate | 18% strongly agree<br>73% agree<br>9% neither agree or disagree |
| The project helped you to develop problem solving and critical thinking skills, and ability to think independently | 36% strongly agree<br>64% agree |

## 4. CONCLUSION

This paper describes our experiences teaching information security using the approach of case studies. Two case studies were developed for teaching physical security and security policies. They were taught in the "Fundamentals of Information Assurance" course in the Spring 2010 semester. Each case study includes learning objectives, case description and case discussion questions. The case discussion questions were mapped to Bloom's and Fink's taxonomies. Survey results show that most students agree that the case studies helped them to relate classroom learning to real-life experiences, increased their interest and motivation in learning information security, and were beneficial for their future career. One case study was also 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 study. 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 information assurance.

## 5. ACKNOWLEDGEMENT

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

## 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, accessed on June 1, 2010.

[2] *Bloom's Taxonomy*, available at: http://www.officeport.com/edu/blooms.htm, accessed on June 1, 2010.

[3] Fink, L. Dee. What is Significant Learning? available at: www.wcu.edu/WebFiles/PDFs/facultycenter_SignificantLearning.pdf, accessed on June 1, 2010.

[4] Whitman, M.E. and Mattford, H.J. *Principles of Information Security 3rd Edition*, Thomson Course Technology, 2009.

[5] SANS Infosec Reading Room – Physical Security, available at: http://www.sans.org/reading_room/whitepapers/physcial/, accessed on June 1, 2010.

[6] How Cisco IT controls building security over the enterprise WAN, Cisco IT case study: Enterprise network building security, available at: www.cisco.com/web/about/ciscoitatwork/downloads/ciscoitatwork/pdf/Cisco_IT_Case_Study_Enterprise_Access_Control.pdf, accessed on June 1, 2010.

[7] Scarfone, K. and Hoffman, P. Guidelines on firewalls and firewall policies, National Institute of Standards and Technology Special Publication 800-41, available at: http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf, accessed on June 1, 2010.

[8] Security Policy: North Carolina Agricultural and Technical State University Information Security Plan, available at: www.ncat.edu/~cit/policies/information_security_plan.pdf, accessed on June 1, 2010.

[9] Security Policy: Griffith University security policy. November2002, available at: www.griffith.edu.au/ins/org/policies/content01.html, accessed on February, 10, 2010.

[10] Security Policy: Sample Backup policy, available at: http://www.comptechdoc.org/independent/security/policies/backup-policy.html, accessed on June 1, 2010.

[11] SANS Reading room. Sample Communication Policy, available at: www.sans.org/resources/policies/Communications_Equipment2.pdf, accessed on June 1, 2010.

[12] SANS Infosec Reading Room Sample Issue specific policies, available at: http://www.sans.org/resources/policies/, accessed on June 1, 2010.