https://doi.org/10.48009/3_iis_2015_164-171

Issues in Information Systems
Volume 16, Issue III, pp. 164-171, 2015

ENGAGING A DIVERSE STUDENT AUDIENCE IN AN INFORMATION SECURITY COURSE

Lynn R. Heinrichs, Western Carolina University, lrheinrichs@email.wcu.edu

ABSTRACT

The purpose of this paper is to discuss the author's experiences in developing activities to engage a diverse student audience in a junior-level information security course. The demographics of the course have changed over the last few years to include students from a wide-range of programs. While hands-on lab manuals are available for teaching information security courses, they tend to focus on technical exercises. Neither do lab manuals always align well with primary textbook content organization. The paper describes several activities the author has developed and used within the context of course learning outcomes to engage an increasingly diverse audience.

Keywords: Information Security Course, Instruction, Student Engagement, Activities, Assignments

INTRODUCTION

After a curriculum change several years ago at the author's institution, the former "network design and security" course was transformed into an "information security" course. While there is overlap between the two courses, they are also very different with network security often seen as a subset of information security. As a result, the audience of students interested in taking the course also changed with broader representation of students from majors outside of the department, particularly in business.

The change in course focus and audience required some serious rethinking of how to engage students. Students could take the course by satisfying one of three prerequisites that included the introductory information science course, the first computer science course, or management information systems. Additionally, a student without one of the prerequisites could request permission to take the course. The activities designed to engage students needed to have appeal to a broad-range of backgrounds and interests, but still be meaningful within the context of the course.

The purpose of this paper is to discuss the author's experiences in developing activities to engage a diverse student audience in a junior-level information security course. The course is required for majors in the information science program and an elective for minors. However, curricular changes in recent years have opened the course to other audiences. The experiences described in the paper are useful to those that currently teach an information security course or are considering the inclusion of such a course in their curricula.

INFORMATION SECURITY TOPICS AND RESOURCES

The Information Security Common Body of Knowledge (CBK) as defined by International Information Systems Security Certifications Consortium (ISC^2) includes the following areas [4]:

- Security Management Practices
- Security Architecture and Models
- Business Continuity Planning
- Law, Investigations, and Ethics
- Physical Security
- Operations Security
- Access Control Systems and Methodology
- Cryptography
- Telecommunications, Network, and Internet Security
- Application Development Security

Professional certification tests offered by the ISC^2 are based upon the CBK. Such breadth and depth is beyond an introductory information security course, even at the junior level; however, the CBK does serve as a meaningful guideline for judging topical relevancy.

For the purpose of teaching the information security course, the author has relied on Whitman and Mattord's textbook, *Principles of Information Security* [7], which touches on many of the CBK topics. The organization of content in the textbook does not require any technical understanding until Chapter 6, at which point firewalls and VPNs are presented. The chapter assumes knowledge of TCP/IP concepts which can be introduced to students using supplemental materials.

Given that data breach stories appear in the media daily, information security should be a dynamic and exciting course for students. However, the presentation of content in an information security textbook can be dry, especially to a millennial audience. The author has worked diligently to identify and/or design engaging activities that students can participate in during class-time.

DESIGNING INFORMATION SECURITY ENGAGEMENT ACTIVITIES

Engaging students from diverse backgrounds can be challenging. Students majoring in computer or information science often want to focus on honing technical skills while non-majors may prefer to apply their managerial competencies. Hands-on information security lab manuals are available that can serve as supplemental textbooks [6]. However, the exercises in these manuals are more technical in nature and do not necessarily follow the content organization of the primary textbook.

The diversity and size of the audience of the author's information security course has evolved over three offerings (see Table1). The first offering took place during the transition of the curriculum from CIS to Information Science; students in essence all came from the same background, but had the option of declaring either major. By the time of the second offering, the curriculum had completed its transition, and students enrolled in the course were information science majors or minors. The minors primarily came from the business school. For both the first and second offerings, the information security was taught in a specialized classroom that was originally designed for a network course. The classroom was conducive to exercises that needed specialized software or infrastructure setups.

In the security course's third offering, a substantial change in audience size and background occurred due to three curricular changes: (1) the Computer Science major accepted information security as an elective; (2) the Management major in business approved the course as an elective; and (3) the University's General Education committee approved the course as an upper-division elective for general education requirements. As shown in Table 1, the enrollment took off. One complication of the larger enrollment was that the course could no longer be taught in the department's specialized network. With 24 students, the course was moved to a general-purpose, computer classroom. With a more diverse audience and a different environment, a new approach to student engagement was necessary.

Table 1. Information Security Enrollment Summary

Offering	Enrollment	Student Composition
S2013	14	Old CIS and New Information Science Majors
S2014	11	New Information Science Majors and Minors
S2015	24	Information Science Majors and Minors, Computer Science Majors, and Management Majors

Charting a New Approach

The learning outcomes for the information security course are as follows:

1. Describe the scope, evolution, and importance of information security in today's organizations.
2. Identify common threats to information security and attacks associated with those threats.

3. Explain the roles of laws, regulations, policies, and codes of ethics in achieving a secure environment.
4. Critique policies and plans related to information security.
5. Apply components of risk management (risk identification, risk assessment, or risk control) to information security problems.
6. Select appropriate technologies methodologies for implementing an information security solution.
7. Effectively communicate information security ideas and contribute to a team project.

The course blends both managerial and technical content. Ensuring that students have the necessary prerequisite skills for participating in activities or completing assignments is essential to learning. One of the consequences of transitioning from the old CIS program to the new Information Science major was the loss of the network course. Basic network concepts are essential for understanding information security technologies. Therefore, to ensure that students are adequately prepared for studying information security technologies, the author incorporates a three-week primer on network topics such as TCP/IP, IP addressing, wired vs. wireless networks, and connecting devices.

Table 2 summarizes the engagement activities the author has designed to support the learning outcomes of the course. As a point of clarification, readers will note that there are no activities tied to learning outcomes one and seven. For learning outcome one, an exercise related to confidentiality, integrity, and availability recommended by the textbook authors is used during class. For learning outcome seven, students propose and complete a comprehensive course project.

Table 2. Learning Outcomes and Engagement Activities

Related Learning Outcome	Outcome Focus	Engagement Activity	Activity Deliverable
2	Identify Threats and Attacks	Information Security Blog Post	250-400 Word blog-post entry (graded)
3	Describe legal, ethical, and professional issues	Documentary Discussion	Written responses to thought questions accompanying documentary discussion guide (graded)
5	Apply components of risk assessment	Simple TVA (Threat, Vulnerability, Asset)	Excel workbook with threat, vulnerability, and information asset valuations (graded)
4	Critique policies and plans	Security Policy Wiki	Small group presentations and critiques done in class (not graded)
6	Select security technologies: firewall features	Firewall Emulator Configuration	Document containing screenshots firewall modifications (graded)
6	Select security technologies: cryptography	Cipher Practice	In-class Excel activity and discussion (not graded)

More information about the activities and deliverables is described below. Some activities in Table 2 can take a substantial amount of time and, depending on the length of a class period, may require both in-class and out-of-class time to complete. If an activity is best served by continuing work outside-of-class, the author generally grades the assignment. For in-class activities, students need access to computers with Internet connectivity.

Threats and Attacks: An Information Security Blog Post

The IT staff at the author's university maintains an information security blog to raise community awareness of information security issues. As one early activity in the course, students propose and develop blog posts of about 250 – 400 words relating to information security threats and attacks. In addition to grading the blogs, the author

shares the blogs with the IT staff. The IT staff reviews the blog posts and selects several to use. If a student's blog post is published, he/she receives extra credit.

While the author benefits from a willing IT staff and existing blog, this activity could easily be adapted as a semester-long, class project. Students working in small groups could be assigned responsibility for creating a blog and making regular posts as part of a security awareness effort for their campus.

Legal, Ethical, and Professional Issues: A Documentary Discussion

There are many excellent films and documentaries that can generate discussion on legal, ethical, and professional issues. *Terms and Conditions May Apply* is a 2013 documentary from filmmaker Cullen Hoback that focuses on user privacy. The documentary Web site provides a discussion guide [1] with links to video clips, related activities, and discussion questions on the following themes:

- "You Agreed to the Following"
- "We May Use Your Personal Data"
- "We May Share Your Information with the Government"
- "Your Information is "Anonymous"
- "We May User Your Data to Prevent"

The author has used the activities and discussion questions for both in-class and out-of-class assignments. The documentary itself has received mixed reviews from various film critics, and can be a bit of a sleeper if watched in its entirety. One advantage of the discussion guide format is that the actual amount of time watching video clips is limited and can be done in advance of classroom discussion.

Risk Assessment: A Simple TVA Worksheet

The risk assessment process involves identifying vulnerabilities between information assets and threats. A risk rating or score is assigned to each specific information asset and is used to determine the relative risk introduced by each vulnerable information asset. One approach for completing the process is to build a TVA (threat-vulnerability-asset) worksheet [7].

TVA worksheets can be very large and cumbersome to construct; yet, the hands-on experience of building such a worksheet is critical for a student's understanding of risk assessment. After conducting a Web search for TVA examples, the author found a simple model used by FEMA for site risk assessment [2] and adapted it to the information security process.

The TVA workbook, consists of four worksheets (Figure 1a). Students begin by identifying information assets for a real-world scenario (Figure 1b) and determining a system for assigning a value score of 1 – 10. (Note: The sample shown illustrates information assets for the classroom computer lab.) Next, the students identify related threats from several threat categories presented in the textbook, and assign a threat value of 1-10 (Figure 1c) with a note of clarification. For each asset and threat combination, the students then determine a vulnerability rating of 1-10 and justify the rating by including a comment (Figure 1d).

The final worksheet calculates a risk score product for each asset, threat, and vulnerability combination. Cell references link the source ratings to the final worksheet. Risk score categories of Low, Medium, and High are defined (e.g. 1-64 is Low Risk), and conditional formatting is applied to reinforce the category assignment (green for Low, yellow for Medium, and red for High).

Security Policy: A Group Wiki Exercise

According to Whitman and Mattord [7], a "quality InfoSec program begins and ends with policy." Most students are at least vaguely familiar with the policies that govern information security at their institutions. One way to help

them understand the complexities of developing effective policies is to task them with collaboratively writing a policy.

For this exercise, students are divided up into small groups of two or three. In advance of class, a Moodle wiki is created with basic assignment instructions and links for each group to start their own policy page. Since the department maintains two labs that are accessible to students, an easy problem to address is the development of an acceptable use policy for one of the labs. After students have developed their policies, each group's effort can be shared with the rest of the class.

Figure 1a. Create TVA Workbook with Four Sheets

Information Asset Ratings

	Asset Score	Importance to Mission	Importance to Revenue	Expense to Replace
Point Distribution	10	3	4	3
Student Computers	7	3	1	3
Storage Cabinet	1	0	0	1

Figure1b. Identify Assets and Valuation (1-10)

Threat Value Ratings

Information Asset	Software Attacts	Rating	Theft	Rating	Espionage/Tresspass	Rating	Human Error	Rating
Student Computers	Virus downloaded	6	Physically taken from room	5	Unauthorized login	4	Drink spilled on computer	4
Storage Cabinet	Not really applicable	1	Items in storage cabinet taken from room	2	Lock on cabinet drawer is picked and contents examined	3	User leaves cabinet door unlocked	3

Figure 1c. Identify Threats and Threat Value (1-10)

Vulnerability Value Ratings

Information Asset	Software Attacts	Rating	Theft	Rating	Espionage/Tresspass	Rating	Human Error	Rating
Student Computers	Anti-virus software up-to-date	5	Combination on door, but sometimes	4	Users generally do not share login information	3	Most drinks are covered	4
Storage Cabinet								

Figure 1d. Determine Vulnerability Values (1-10)

	Information Security Threats			
Information Asset	Software Attacts	Theft	Espionage/Tresspass	Human Error
Student Computers	210	140	84	112
Asset Value	7	7	7	7
Threat Rating	6	5	4	4
Vulnerability Rating	5	4	3	4
Storage Cabinet	1	6	9	6
Asset Value	1	1	1	1
Threat Rating	1	2	3	3
Vulnerability Rating	1	3	3	2

Figure 1e. Calculate Risk Score (Asset x Threat x Vulnerability

Security Technologies: Router/Firewall Emulator Configuration

On-line emulators from a wide-range of manufacturers are available for exploring the features of network equipment. These tools are useful to get the experience of configuring different types of devices without having access to a specialized laboratory. This became a critical consideration once the enrollment of the author's information security course expanded beyond the department's specialized lab capacity.

Figure 2a shows an actual Linksys LRT224 router with WAN and LAN ports that has both firewall and VLAN functionality. Figure 2b shows the main configuration tab for the router's online emulator [3]. Figure 2c contains an excerpt from a hands-on exercise to add firewall configuration rules. Note: The exercise parallels a YouTube tutorial on configuring a similar Linksys router [5].

Emulators have their downsides. As students are completing an exercise, changes to the settings are temporary. Work is often loss just moving from one screen to another. Likewise, changes cannot be tested, so students cannot determine whether or not their choices were appropriate. For the purpose of checking student work, screenshots are an alternative.

Figure 2a. Linksys LRT224 Router

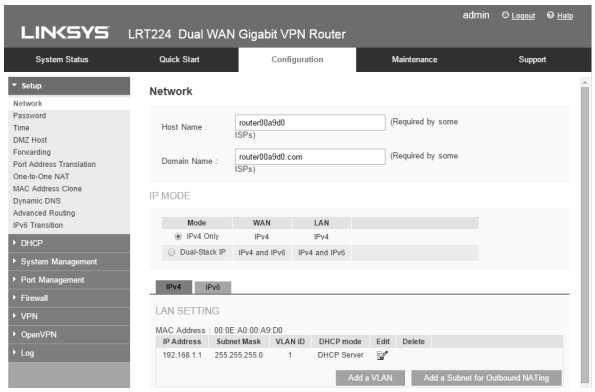

Figure 2b. LRT224 Emulator Configuration Tab

LAN¤	Device¤	IP·Address¤
PortID1¤	Email·Server¤	192.168.1.105¤
PortID2¤	Web·Server¤	192.168.1.110¤
PortID3¤	Database·Server¤	192.168.1.115¤
PortID4¤	¤	¤

¶

1.→ ·Click·on·the·Access·Rules.··There· are·three·rules·currently·configured·in·the·firewall.··**Take· Screenshot2**.¶

a.→ Below·Screenshot2·in·your·document,·briefly·explain·the·purpose·of·each·of·the·three· rules·configured·by·default.¶

2.→ Click·on·the·button·to·Add·a·new·rule·that·allows·inbound·SMTP·traffic·to·the·email·server·from· any·location.·**Take· Screenshot3**·BEFORE·hitting·the·Save·button·(the·Save·will·actual·reset·your· entries).¶

3.→ Add·another·rule·that·allows·inbound·HTTP· traffic·to·the·Web·server.··**Take· Screenshot4.**¶

4.→ Add·another·rule·that·allows·remote·desktop·connections·to·the·Database·Server·on·TCP·port· 3389.··This·is·not·a·standard·service,·so·before·you·can·set·up·this·rule,·you·must·click·on·the· Service·Management· button·and·set·up·the·service·first.··After·clicking·on·the·button,·enter·the· following·information:··RDC·for·the·service·name,·TCP·for·the·protocol,·and·3389·for·the·starting· and·ending·port.··Click·the·Add·to·List;··scroll·down·to·verify·that·RDC·has·been·added·to·the·list.··· **Take· Screenshot5.**· ·Note:··once·you·return·to·the·access·rule·entry·form,·the·RDC·list·entry·will· not·be·saved.··So,·be·sure·to·take·Screenshot5·after·updating·the·list.¶

Figure 2c. Excerpt from Hands-on Exercise Configuring Firewall Rules

Security Technologies: Cipher Practice with MS-Excel

Because business students seem to relish opportunities to work with spreadsheets, any activity that involves Excel goes over well. With the cipher practice exercise, students have an opportunity to learn some new Excel functions while learning basic cipher techniques. Figure 3 shows a substitution and transposition cipher using CHAR, CODE, and MID functions. The XOR cipher also uses CHAR, CODE, and MID as well as DEC2BIN, BIN2DEC, and IF. Note that the author's institution was still using Excel 2010 at the time of this paper submission; the XOR cipher should be simpler with the BITXOR function introduced in Excel 2013.

As the author was quickly reminded during her first attempt at doing the cipher practice in class, student comfort-level with Excel can vary greatly depending on major. Some students might need a refresher before beginning this exercise.

1										
2		Cipher Practice								
3										
4		**Cleartext***	**cat**			**Substitution Cipher**	dbu	(add 1 to letter value)		
5		**Keyword**	**dog**							
6						**Transposition Cipher**	tac			
7										
8						**XOR**				
9						**Cleartext (ASCII)**	99	97	116	
10						**Keyword (ASCII)**	100	111	103	
11						**Cleartext (Binary)**	01100011	01100001	01110100	
12						**Keyword (Binary)**	01100100	01101111	01100111	
13						**XOR**	00000111	00001110	00010011	
14						**Encrypted (ASCII)**	7	14	19	
15						**Encrypted Text**	•	♬	!!	
16										
17										
18		**Note: To keep this simple, just assume the clear text phrase is exactly three letters*								

Figure 3. Cipher Practice with Excel

Any Information Security Topic: Guest Speakers

Guest speakers, whether in person or by Skype, add a new dimension to class discussions. The author has relied on guest speakers, such as the following, to bring real-world experiences to textbook topics:

- *Careers*. A member of the IT staff who had completed a master's degree in information security describes her career path.
- *Identity theft*. A faculty member from another institution who experienced identity theft describes her personal experiences addressing its consequences.
- *IT auditing*. A recent alum who landed a job as an IT auditor describes the IT auditing process and its intersection with information security.
- *Data sensitivity*. An information security specialist from another institution who recently completed a professional certification discusses a data classification project.
- *Security planning*. The Chief Information Office (CIO) for the institution describes the security planning process and the challenges unique to academic environments.

In preparation for a guest speaker, students are assigned relevant readings and research questions to prepare and submit in advance. Prior to the speaker's presentation, the research questions are discussed and students take responsibility for questioning the speaker in specific areas. Following the presentation, the class discusses what they have learned from the guest speaker and how it relates to what they have learned in the course. It has not been the author's practice to incorporate exam questions related to a guest speaker.

CONCLUSIONS AND FUTURE DIRECTION

The purpose of this paper was to discuss the author's experiences in developing activities to engage a diverse student audience in a junior-level information security course. The author has found over the last few years that supplemental lab manuals do not always provide the types of exercises that work well when students represent a broad range of backgrounds. Neither do lab manuals always align well with primary textbook content organization.

While engaging diverse students has been challenging, the outcomes have been rewarding. Informal, in-class feedback from students has been supportive of the activities used for teaching the information security course. However, while the activities engage students and make for more interactive class meetings, their value in preparing students for formal exams has yet to be established. As a next step in evaluating the effectiveness of the activities for learning, the author plans to develop a more formal assessment process.

REFERENCES

1. Active Voice (2014). *Terms and Conditions May Apply Discussion & Activity Guide*. Retrieved from tacma.net/TACMAGuide.pdf
2. FEMA (n.d.). *Building Design for Homeland Security: Unit V Risk Assessment/Management*. Retrieved from http://www.fema.gov/pdf/plan/prevent/rms/155/e155_unit_v.pdf
3. Linksys (n.d.). *Linksys LRT224 Dual WAN Gigabit VPN Router*. Retrieved from http://ui.linksys.com/files/LRT224/1.0.0.07/cgi-bin/welcome.htm
4. Merkow, M. and Breithaupt, J. (2006). *Information Security: Principles and Practices*, New Jersey: Pearson Education, Inc.
5. Vanderpool, L. (2013). *Home to Business Networks Part 4 Understanding Firewalls*. Retrieved from https://www.youtube.com/watch?v=rcEiezD7NqQ
6. Whitman, M. and Mattord, H. (2014). *Hands-on Information Security Lab Manual*, Boston: Course Technology, Cengage Learning.
7. Whitman, M. and Mattord, H. (2012). *Principles of Information Security*, Boston: Course Technology, Cengage Learning.