2016

# Hacking to Prepare Undergraduate Students for Cybersecurity Attacks

Lori Baker-Eveleth
*University of Idaho*, leveleth@uidaho.edu

Stefanie Ramirez
*University of Idaho*, sramirez@uidaho.edu

# Hacking to Prepare Undergraduate Students for Cybersecurity Attacks

Lori Baker-Eveleth
College of Business and Economics
University of Idaho
leveleth@uidaho.edu

Stefanie Ramirez
College of Business and Economics
University of Idaho
sramirez@uidaho.edu

**Abstract:**

Businesses are dependent on computer networks and information systems (IS). Much of the data businesses store are internet or cloud-based. This increases the challenge of protecting data that may not be stored in the physical facilities of a business. With the projection of more cyberattacks and threat of cloud-based data, preparing undergraduate students to recognize vulnerabilities in a system is a needed skill for the future. A medium-sized, northwest-based university with limited resources is piloting online labs with competitions to enhance students' knowledge and experience.

**Keywords**: security, cyber competitions, IS curriculum

## I. INTRODUCTION

St. Jude Medical stock dropped 2.5% in a day when the company announced its cardiac devices were vulnerable to cyberattacks. Hotel giants Marriott and Hyatt found malware on its system and customer credit card information may have been retrieved by hackers. Eddie Bauer's retail stores point-of-sale systems were infected with malware affecting customer credit card information. Foreign hackers are suspected of penetrating two U.S. state election databases. All of these reports occurred in a one-week period of time in August 2016. As the number and frequency of the attacks increases, the Federal Bureau of Investigation (FBI) ranks cybercrime as a top priority. Preparing students for these destructive cyberattacks is more important now than ever.

Businesses are dependent on computer networks and information systems (IS). Much of the data businesses store are internet or cloud-based. This increases the challenge of protecting data that may not be stored in the physical facilities of a business. With the projection of more cyberattacks and threat of cloud-based data, preparing undergraduate students to recognize vulnerabilities in a system is a needed skill for the future (Abawajy, 2014; Jang-Jaccard & Nepal, 2014).

To address the growing cyber threats, many information system programs are developing cybersecurity courses to include in the curriculum (Cram & D'Arcy, 2016; Harris & Patten, 2015; Mabece, Futcher, & Thomson, 2016; Woodward, Imboden, & Martin, 2013).

## II. LITERATURE REVIEW

The growing threats of a cyberattack leads to the need to prepare undergraduate students for the ever changing environment. Woodward et al. (2013) implemented a new security course to two networking courses to begin a security program. The curriculum has expanded to ten courses for the program. The courses provide both theoretical and hands-on experience and also pair with student organizations and industry partners. They were able to create labs using virtualization technologies to offer courses online further expanding the programs reach. Woodward et al. also

suggest developing an information security course at the freshman level to capture and develop knowledge early in a student's academic career.

Harris and Patten (2015) provided a case study, in a resource constrained environment, to provide information technology undergraduate students with the knowledge and skills needed without increasing courses or credits. Prior to the new curriculum format students in the program had one course that provided an overview of security topics but wasn't addressing the emerging needs of the workplace. The faculty re-designed their strategy to incorporate security in all of the courses in the program. By doing this, no new courses were added or raises to the required credits to graduate for a student.

In medium and small universities, it is challenging to add courses and credits to an already full curriculum. On our campus we have an existing cybersecurity center but the only students who can participate are computer science students. We wanted to add cybersecurity to our information systems curriculum to expose more students to the topic and to convince students outside of the typical technology path to learn more about cybersecurity. Using these two examples as a foundation, our information systems program chose an online, competition-based approach to enhance the security curriculum.

## III. METHODOLOGY

Our medium-sized, northwest-based university is constantly addressing fading state funding and flat university enrollment. The ability to add required courses to the curriculum or expanding credits for the program were not a feasible option at this time. Without the ability to modify the curriculum, an alternative approach was proposed to address the issue and piloted last year.

An online cybersecurity class was piloted in the fall of 2015 which included a cyber-competition. Students were recruited via word of mouth from faculty in the IS area. The student participants ranged in age and experience from senior information systems to freshmen with no declared major. Initially eleven students enrolled in the course and competition and ten students finished.

As part of the online course, student's completed virtual labs, similar to what is discussed in Woodward et al. (2013) paper. The virtual labs were originally developed by funding from the National Science Foundation's Advanced Technological Education program with the Department of Undergraduate Education and the Center for Systems Security and Information Assurance (CSSIA) at Moraine Valley Community College. The organization providing the labs and the competition is the National Cyber League. It provides a training ground for students to learn cybersecurity skills with little prior knowledge. We provided the course and competition to students as a one-credit course in which they were required to participate in at least one of the two online competitions.

The online class provided labs via virtual machine template and runs from October until the beginning of the competitions in the end of November. After students completed most of the labs, they participated in a pre-season game to determine his or her level of knowledge. Student participants then competed in two individual competition games of "Capture the Flag" using their knowledge of ethical hacking and multipurpose security. Using a "gym" and "stadium" enhanced the game feeling for students as they compete against other students in password cracking, wireless access exploitation, and network traffic analysis. For example, during the game in order to capture a flag, a student would need to understand packet capture on network traffic and identify the IP address of a request, identify the server address, and the IP address of the server.

## IV. PRELIMINARY RESULTS

Student participants completed a pre-survey prior to the competition and a post-test survey following the competition. The pre-test assessed student's base level of knowledge on

cybersecurity concepts (see Table 2 for example items). Students then participated in the virtual labs focusing on ethical hacking and cybersecurity concepts related to the CompTIA certification. Following the labs and competition experience, students took, and will take, the post-test to assess their learning. This was, and will be, used to compare and determine what they learned between the pre- and post-test experience.

Demographic information on the student participants is summarized in Table 1 for the fall 2015 and 2016 groups. Additionally, in both pre- and post-tests, students acknowledged their overall computer knowledge and skill in information technology (IT) and security. The pre-test results indicated that 64% of the participations had previous experience with IS or IT in 2015 and 57% in 2016; 30% had previous experience with information security or cybersecurity in 2015 and 43% have previous cybersecurity experience (see Table 2).

In addition, most of the students felt very comfortable dealing with managing files on their computer, seeking out help for problems related to information systems but weren't not as confident in handling virus infected files or getting rid of spyware. This supports our assumption that students could use more exposure to cybersecurity topics.

From the post-survey results for 2015 only one of the student's post-test scores improved on security knowledge. Interestingly, 30% of the student's indicated a decrease in confidence in handling viruses and protecting information systems. In discussions with the students following the competitions, many were surprised at how quickly they needed to act in a cyberattack and how important it was to have the correct tools to fight an attack.

The second instance of the online class and competition is currently in session. Additional data will be collected using the same pre- and post-survey as well as the outcome results from the performance of the competition. Currently, fourteen students are enrolled representing a wide range of ages and experiences (see Table 1). More data will be collected regarding the change in students' confidence and experience using cyber hacking tools to further develop students' knowledge. Additionally, longitudinal data will be collected for students that repeat their participation in the cybersecurity courses and how this affects retention of knowledge and self-assessment. Scoring information from participation in competition will also be used to analyze how previous IS/IT experience changes competition outcomes (how much does previous experience help?) and to what extent these outcomes are improved with repeat participation in the national competition. Preliminary results from the second experience will be presented.

## V. REFERENCES

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology,* 33(3), 236-247.

Cram, W. A., & D'Arcy, J. (2016). Teaching Information Security in Business Schools: Current Practices and a Proposed Direction for the Future. *Communications of the Association for Information Systems, 39*(1), 32-51.

Harris, M. A., & Patten, K. P. (2015). Using Bloom's and Webb's Taxonomies to Integrate Emerging Cybersecurity Topics into a Computing Curriculum. *Journal of Information Systems Education, 26*(3), 219-234.

Mabece, T., Futcher, L., & Thomson, K.-L. (2016). *Towards using pervasive information security education to influence information security behaviour in undergraduate computing graduates.* Paper presented at the CONF-IRM 2016, Cape Town, South Africa.

Woodward, B., Imboden, T., & Martin, N. L. (2013). An undergraduate information security program: More than a curriculum. *Journal of Information Systems Education, 24*(1), 63-70.

Table 1. Demographics from 2015 and 2016

| Demographics | 2015 | 2016 |
|---|---|---|
| Gender | 100% male | 33% female<br>66% male |
| Age | 19- 25 age range<br>21 average age | 20-42 age range<br>23.9 average age |
| Class Standing Count | | |
| Sophomore | 3 | 1 |
| Junior | 2 | 6 |
| Senior | 6 | 7 |
| Graduate Student | | 1 |
| Experience within the field of Information Systems or Information Technology | 64% | 57% |
| Year in School | | |
| Major | | |
| Accounting | | 2 |
| Information Systems | 11 | 11 |
| Other | | 2 |
| Number of Students Completed the Pre-Test | 9 | 14 |

Table 2. Pre-Survey Items

| Items |
|---|
| Do you have any experience in the fields of Information Security or Cybersecurity? |
| Students rated the following statements based on their confidence in completing tasks* |
| Handling virus infected files |
| Getting rid of spyware |
| Understanding terms/words relating to information security |
| Learning the method to protect my information and information system |
| Managing files in my computer |
| Setting the Web browser to different security levels |
| Different programs to protect my information and information system |
| Learning advanced skills to protect my information and information system |
| Getting help for problems related to my information security |
| Using the user's guide when help is needed to protect my information and information system |
| Updating security patches to the operating system |

*7-point Likert Scale (Strongly Disagree, Disagree, Somewhat Disagree, Neither Agree or Disagree, Somewhat Agree, Agree, Strongly Agree)