Cyber Security for Everyone – An Introductory Course

Conference Paper · January 2017

CITATION
1

READS
3,312

1 author:

Marc Dupuis
University of Washington Bothell
28 PUBLICATIONS **110** CITATIONS

SEE PROFILE

INTRODUCTION

Cyber security focused degrees have become more popular in the past several years; however, there remains a dearth of courses in cyber security for the non-major. If humans really are the weakest link within cyber security, then this gap within our education system must be addressed immediately.

In this paper, we discuss the development of a cyber security course for non-majors. It is a foundational course intended to educate individuals on the various components of cyber security and privacy so that they can make more informed decisions as consumers. While the course discussed herein involves an undergraduate course in college, we acknowledge the need for similar courses within our primary and secondary education systems, among other venues (Baumann, 2016). The approach outlined here could serve as a model for courses offered in other settings.

The remainder of the paper is organized as follows. First, we discuss the need for the masses to be educated on the basics of cyber security. These basics include backing up data, being suspicious of emails and other phishing pathways, keeping current anti-malware software installed on all computing devices, and using great caution with respect to the amount and type of personal information that is shared.

Second, we detail the approach taken in the development of an undergraduate course in cyber security. This approach included developing curriculum relevant to non-technical majors. For example, labs were developed that had them perform actual protective measures on their personal computers, such as installing software that performs automatic backups of their data to the cloud.

Third, we discuss the results of two iterations of the introductory cyber security course that was developed. This includes feedback from students and lessons learned. In particular, we discuss one significant gap that was not able to be fully remedied—the need for a textbook appropriate for the target audience.

Fourth, we place the curriculum developed for this course within the context of Bloom's Taxonomy. This includes examples that illustrate how all of the levels of Bloom's Taxonomy are engaged by the activities developed for this course.

Fifth, we discuss the benefits this type of course has to various stakeholders, such as students, STEM programs, colleges, and society as a whole.

Finally, the implications of our work are discussed, including possible next steps. These next steps could involve adapting the curriculum to secondary school students and developing a textbook that is suitable for both college and secondary school students.

A discussion on the need to educate the masses on the basics of cyber security follows.

EDUCATING THE MASSES

The cyber security and privacy threat is real. It is real for the financial sector, government, military, public safety, critical infrastructure, and it is real for the average every day person (Choo, 2011). The average person engaging in online behavior at home poses a cyber security risk and this is most often due to a lack of knowledge, skills, or abilities. For example, some estimates suggest that 25 percent or more of home computers have malware on them with up to 60 percent of these also serving as botnets (Creeger, 2010; Young, 2008).

It is important that we continue to educate, train, and develop cyber security professionals that can protect our nation and our people. This includes developing programs that assist faculty in doing this the most effective way possible (Namin, Hewett, & Inan, 2015) or developing forums in which curriculum ideas can be exchanged (Frincke & Bishop, 2004). However, the focus has too often been exclusively on this component rather than educating the masses on what they can do to protect themselves from various cyber security and privacy threats they encounter each and every day (e.g., (M. E. Locasto, Ghosh, Jajodia, & Stavrou, 2011; M. Locasto & Sinclair, 2009; Schneider, 2013)).

While the focus has remained mostly on cyber security professionals and organizational users, there is some evidence that the need for a broader cyber security education is being recognized. This includes developing awareness programs and some type of enforcement mechanism for home users via their Internet Service Providers (ISPs) (Kritzinger & von Solms, 2010). There are of course challenges associated with such an approach. How many ISPs desire additional responsibilities and costs? However, if they can be shown how it may actually reduce costs then this remains a possibility.

Another approach that could be taken is to require all students to take an introductory cyber security course or a general information technology course with a moderate focus on cyber security. This works well for some institutions, such as West Point, that have a structure and curriculum conducive to such an approach (Sobiesk, Blair, Conti, Lanham, & Taylor, 2015). The heavier focus on technical majors and courses of study is likely to foster rather than hinder such courses, especially if they are required.

At traditional liberal arts colleges and universities, this may prove to be more difficult. Nonetheless, a comprehensive cyber security course is multi-disciplinary by its very nature and there are opportunities here that can be attractive to other disciplines. For example, a course at one university introduces a multi-disciplinary

approach to intelligence analysis (Kam & Katerattanakul, 2014). Leveraging the social and behavioral sciences into our cyber security and privacy curriculum also makes a lot of sense since a large part of the problem is the human factor (Mann, 2012; Pfleeger & Caputo, 2012; Pfleeger, Sasse, & Furnham, 2014; Sasse, Brostoff, & Weirich, 2001). The needs for other approaches has also been acknowledged by the Department of Homeland Security and other entities (Kessler & Ramsay, 2013).

While an introductory cyber security course as a requirement for all may be appealing for many reasons—that is not what we are proposing here. Rather, we are detailing the development of a course that serves as an elective for undergraduate students that fulfills a general education requirement.

Next, we discuss the development of a comprehensive introductory cyber security course for non-majors.

AN INTRODUCTORY CYBER SECURITY COURSE

In this section, we discuss the development of an introductory cyber security course. First, we discuss the student learning goals, followed by an outline of the course and then the process of trying to find an appropriate text book, and finally the assessments and activities developed for this course.

Student Learning Goals

The student learning goals consisted of the following:

- Describe the basic components of computer networking
- Examine the concept of privacy and its legal protections
- Explain the primary concepts involving encryption
- Perform basic computer forensics
- Develop and execute a password management plan
- Describe the social implications of cyber security
- Understand the risks and benefits of social networks
- Conduct various ethical hacking procedures
- Describe the basic ethical considerations related to cyber security

These goals were not all-inclusive; rather, they were designed to be representative of the goals for the students for this course.

Outline of the Course

One challenge in developing a course such as this is to provide enough foundational knowledge in technical concepts without either overwhelming them or inundating them with information that was not relevant to the big picture of how cyber security

and privacy is important to them and what they can do about it. Ultimately, we decided on the following outline of topics in the order illustrated in Figure 1.

	Two-Hour Class Sessions																	
Course Topic	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**
Introduction																		
Computer Networks																		
Cryptography																		
Access Controls																		
Threats and Human Factors																		
Forensics																		
Privacy																		
Ethics and Free Speech																		

Figure 1. Course Topic Ordering and Two-Hour Class Sessions per Topic

The timing and number of two-hour class sessions devoted to a specific topic is denoted by the number and placement of darkened blocks above. Course instruction consisted of interactive lectures, videos, and activities to engage them in the material, such as a Google hacking exercise.

Finding a Text Book

Another challenge encountered in developing this course was finding an appropriate text book for the course content and its audience. Several possibilities were explored, including using text books designed for organizational security, certification courseware, small eBooks that cover certain aspects of the content (Eydie, 2015; Ioannou, 2014; Leanage, 2012; Omega, 2014), as well as developing the content from scratch. Attempts were initially made to develop an appropriate text book from scratch, but given time constraints this proved to be an untenable approach.

With respect to certification courseware, EC-Council has a certification with a book called “Certified Secure Computer User” (“Certified Secure Computer User | EC-Council,” n.d.). At the time, there were two challenges associated with adopting this curriculum: 1) It was outdated, and 2) It did not go into the depth sought for a term-long course. Since that time, it appears they have updated the content of the text. However, similar to most courseware for a certification, the goal is to pass the certification exam; it is not necessarily to learn, practice, and experience the content in a long-term meaningful way. Additionally, there does not appear to be a standalone option to purchase the book.

Ultimately, we decided on a custom eBook which combined chapters from various organizational security texts. While this did accomplish the goal of

providing depth into most all of the desired content areas, the focus on the organization and at times disjointed nature of the eBook makes it less than an ideal long-term solution for this course.

Assessments and Activities

The course consisted of in-class quizzes/activities, exams, a team project, a professional presentation, and lab assignments. The assignment category and its associated weighted grade distributions are presented in Table 1, followed by a description of each assignment category.

Assignment Category	Assignment Type	Weight
In-Class Quizzes / Activities (12-18)	Individual	24%
Lab Assignments (6)	Individual	30%
Presentation (1)	Individual	5%
Exams (2)	Individual	16%
Team Project (5 parts)	Team	25%
Total		**100%**

Table 1. Assignment Categories and Weighted Grade Distributions

In-Class Activities/Quizzes

The in-class activities/quizzes were designed to test them on the reading as well as have them engage in some fun activities. For example, one activity had them build a Caesar cipher wheel and encrypt/decrypt a series of messages.

Another activity we mentioned earlier, Google hacking, had them combine various search engine operators to try and find various types of information, including documents that had potentially sensitive information on them. Figure 2 shows an example of such a search.

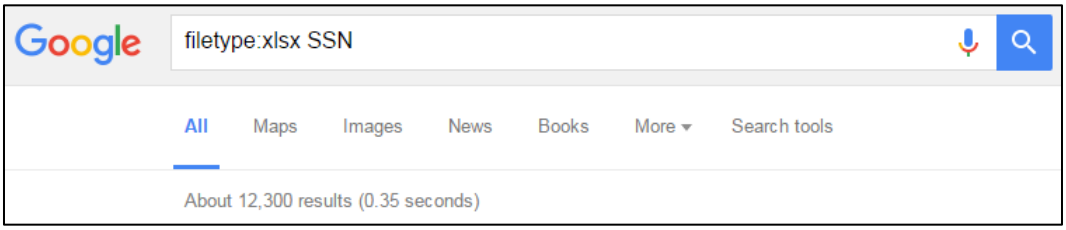

Figure 2. Google Hacking using the filetype operator with the search term SSN

In one case, a student did find something disconcerting. We discussed it in class and drafted an email to the owner of the document informing them of our concerns. They responded and thanked us for notifying them.

Thus, these activities allow students to learn and understand technical, social, and behavioral components of cyber security and privacy, including ethical obligations we each have as part of the broader cyber security community.

Exams

There was a midterm and a final exam during the term. Neither of these exams accounted for a large portion of their grade—8% each. Similar to the reading quizzes, they were designed to ensure a baseline level of knowledge with respect to the terms and concepts covered in class. The questions consisted primarily of multiple choice.

Team Project

The team project provided the students with an opportunity to conduct more in-depth research on a particular cyber security and/or privacy topic of interest to them. The goal was to engage them with many of the components of cyber security and privacy. In order to provide a framework that would allow them to systematically explore a topic, the team project was completed in five stages:

1) Research: Students individually identify at least five research articles and then as a team compile them into a single narrative. At least three of the research articles should come from peer-reviewed sources. A brief primer on searching for articles using the library's database and Google Scholar was provided.
2) Development: Students build on their research from the first stage and create a tri-fold brochure that clearly articulates their research topic in an easily digestible form that is consistent with any other tri-fold brochure. The emphasis here was on the presentation of ideas using bullet points, images, diagrams, and some narrative to convey the key points of the topic they're exploring. This forced them to learn what those key points were before developing a longer narrative in a paper and later in their presentation.
3) Draft of Final Product(s): Students were given a choice between a regular research paper consisting of 3,000 – 4,500 words or a shorter research paper (1,250 – 2,000 words) and a video tutorial/infomercial. At this stage they needed to deliver a very clear outline and plan for their final deliverable(s).
4) Presentation: The students presented their research to the entire class. If they opted for the shorter paper and video option then they would deliver a short presentation and show the video to the rest of the class. The teams were

encouraged to be creative in the videos they made or the presentations they developed. They were encouraged to have fun in how they conveyed important cyber security and privacy topics; thus, keeping their level of engagement much higher than it would otherwise have been.

5) Final Product: Students submitted their final versions of the team project. They were given an opportunity to conduct peer evaluations on one another as well. Peer evaluations were done primarily to identify top performers and those that failed to engage at an adequate level with the effort of the team.

Professional Presentation

In addition to the assignments noted above, each student had to research a cyber security topic of interest to them. They would then present that information to the rest of the class, with or without slides. The purpose was three-fold: 1) Gain in-depth knowledge on a specific cyber security topic; 2) Increase confidence in public speaking, and 3) Learn how to articular complicated cyber security topics to individuals that may have limited knowledge of it beforehand.

Students chose a variety of interesting topics, including the history of cryptography, how public key cryptography works, social media privacy, how to use a password manager to manage one's many passwords, digital forensics, Stuxnet, ransomware, and backing up data, among others. The students were primarily freshmen with little technical background beyond this course, but nevertheless they did a remarkable job of presenting often times complex information in a manner that their classmates could understand and appreciate.

Lab Assignments

Finally, students had six lab assignments throughout the quarter. Each lab assignment included several questions that they must research to find the correct answers to, specific tasks to perform, and finally some self-reflection questions at the end. The idea is for them to perform these lab assignments on their own computers. The general structure of each lab assignment follows:

- Title: The title of the lab assignment reflects the topic the student will be exploring.
- Background: The background section generally includes two to three paragraphs that describe the lab assignment, including the importance of the topic to both them and society at large.
- Goals and Objectives: The goals and objectives specify what the student should learn by completing the lab assignment with key takeaways noted.

- Criteria for Assignment: The criteria indicates how the student will be graded for the lab assignment.
- Requirements: The requirements identify the key items the student must complete in order to successfully achieve the goals and objectives.
- Tasks: The tasks identify how the student will complete requisite requirements.
- Questions: The questions raise important issues related to the lab assignment topic. For example, a question from the lab assignment on digital forensics asks the student to identify what happens when a file is deleted.
- Reflections: The reflection questions are designed to have students think about what they accomplished in the lab assignment, how it impacts them personally, and the importance of the concepts in more general terms.

While learning about cyber security in the course, they are taking proactive measures on their own computers to become more secure. This makes the course more relevant to them and also helps them increase the cyber security posture significantly by the end of the term. Either free or trial versions of software were used for each lab assignment to minimize the cost to the student. The lab assignments included the following:

Lab Assignment 1: Your Cyber Security Posture

Students conduct an 'audit' of their current cyber security behavior and readiness. This includes questions related to their computing devices (e.g., type, OS, version, security software installed, etc.), what files they back up, their home network configuration and how they decide to connect to WiFi networks outside of the home, password management, and social networking.

Lab Assignment 2: Understanding and Using Cryptography

Students install software to learn both encryption and steganography. This includes downloading multiple free software titles that provides full disk encryption, file encryption, and steganography. Students are asked to take screen shots of their activities, encode a message hidden within an image and send it to the instructor, as well as decode a message hidden in an image from the instructor.

Lab Assignment 3: Understanding the Threat Landscape

Students install anti-malware software and run a comprehensive scan on their computer. This includes downloading and installing free anti-malware software that works with their primary computing device (links are provided), running comprehensive scans of their computer with this software, taking a screen shot of

the results, and answering several questions about different types of malware, historical examples of each type of malware, and what it does to a system.

Lab Assignment 4: Digital Forensics, Data Recovery, and Data Protection

Students install software that automatically backs up their computer as well as software that allows them to recover previously deleted files. This includes downloading and installing CrashPlan (local backup is free) and PhotoRec (free photo and file recovery tool). Students were asked to use the photo and file recovery tool and identify anything interesting they found from the scan, including previously deleted files and files they did not know ever existed on their computer in the first place.

Lab Assignment 5: Privacy, Social Media, and Anonymity on the Web

Students install https everywhere, the Tor browser, learn about anonymous email services, and research how well they really know their Facebook friends. This includes visiting a few web sites and noting whether or not https is used, then installing https everywhere on compatible browsers and visiting those same websites again. Generally speaking, students should now see that https is being used, when possible. With respect to their Facebook friends, students had to identify the first 25 friends on their friends list, how long they have known each of them, how well they know each of their friends, whether or not they met this friend in-person prior to becoming friends on Facebook, when they last saw this friend in-person (if ever), the last time they spoke to this person on the phone (if ever), and how close of friends they are with each person.

Lab Assignment 6: Managing Passwords

Students download and install a password manager and configure it appropriately for use. This includes deciding on a password manager that will suit their particular needs and answering several questions about authentication techniques, including the different factors and what is meant by two-factor authentication.

BLOOM'S TAXONOMY

With the aforementioned activities and assessments in mind, it will be helpful to examine them in the context of Bloom's Taxonomy. In a revised version of Bloom's Taxonomy there are six cognitive processes identified: 1) Remember; 2) Understand; 3) Apply; 4) Analyze; 5) Evaluate, and 6) Create (Krathwohl, 2002). This work is based off of the original formulation done half of a century earlier (Bloom, 1956).

These cognitive processes are generally viewed as a hierarchy in which the sixth process, create, is often considered of higher cognitive complexity and abstraction than the first one, remember. As one moves from the lower cognitive processes to the higher cognitive processes he/she moves from simplicity and concreteness to greater complexity and abstraction. While there is a hierarchy, it does not necessarily imply that one level is of greater importance than another; rather, that there is value in designing education curriculum that addresses the processes appropriate for the goals of the course (Case, 2013; Krathwohl, 2002; Krathwohl & Anderson, 2010; Wineburg & Schneider, 2009).

In the next several paragraphs, we will briefly examine how various assessments and activities within the course we designed addressed different cognitive processes found in Bloom's Taxonomy.

Remember

Remembering consists of learning material and establishing it into long-term memory. Recognition and recall are central to this cognitive process (Krathwohl, 2002).

In this course, there were two primary mechanisms used to assess remembering. First, in-class quizzes held them accountable for the required readings. These quizzes were relatively straightforward for students if they had done the reading, but generally challenging if they had not. Likewise, students did not know in advance if there would be a quiz that day, an in-class activity, or both.

Second, there were two exams throughout the quarter: a midterm and a final. These exams were multiple choice and concerned with the student demonstrating recognition and recall of the primary concepts and terms covered in the course.

Understand

Understanding involves figuring out the meaning of information, including information in the written, oral, and graphical forms. Terms used to describe this process include: interpreting, exemplifying, classifying, summarizing, inferring, comparing, and explaining (Krathwohl, 2002).

In this course, students demonstrated understanding of the material by performing in-class activities, answering questions within the lab assignments, and delivering a presentation on a cyber security topic of their choosing.

For example, one in-class activity had them research information on automated offsite backup software as well as recovery software. Students had to identify the names, pros, cons, and cost of various options and determine which option would be the best for them.

Apply

Applying involves taking information that one knows and understands and carrying out an activity based on this information. Executing and implementing are central to this cognitive process (Krathwohl, 2002).

In this course, we really wanted students to see how cyber security and privacy were relevant to them and their daily lives. Thus, we had them apply various components of what they learned on their own computer and in their own lives.

For example, students used software to recover previously deleted files. They were asked to identify the types of files they found, identify anything surprising they found, and employ the software in the future should the need arise.

In another lab assignment, students installed anti-malware software on their computer and performed a security scan. In each lab assignments and in several of the in-class activities students were applying the information they had learned.

Analyze

Analyzing consists of determining how different parts of something relate to one another and the role each part plays within and between one another and to the whole. Differentiating, attributing, and organizing are central to this cognitive process (Krathwohl, 2002).

In this course, students had to analyze information and activities in various contexts. For example, an in-class activity had them perform Google hacking. They used various operators to see if they could find documents that might be sensitive in nature. By selecting different operators and combining them together, they were able to learn how Google hacking can be effective in exposing sensitive materials.

Another example involves students analyzing the results that the data recovery software provided them with. They had to make a determination on which files were relevant to the process they employed and their overall goals in data recovery. This required careful thought and consideration, as well as some research on the purpose different files served on a computer.

Evaluate

Evaluating consists of students making judgments based on a pre-existing standards and/or criteria. Checking and critiquing are central to this cognitive process (Krathwohl, 2002).

In this course, students conducted several different types of evaluations. This included peer evaluations on the work of their peers, as well as evaluating results from anti-malware scans, data recovery results, and the Google hacking activity.

They had to think critically to determine what the information meant given the context in which it was presented. For example, going through their top 20 Facebook friends and identifying how they know each of them, how well, whether they've met them in person before or not, and how often they communicate with the individual outside of Facebook helped them evaluate how well they really know their Facebook friends. This also led to some proactive measures by some students in the deletion of friends they determined that they did not really know that well at all.

Cyber security and privacy are challenging topics, even for the most experienced professional. There aren't always clear cut answers on whether something is a threat or not or what action to take when presented with certain information. The ability to evaluate what they see in this space is critical for them.

Create

Creating consists of bringing the various components they have learned at any and all of the other cognitive process levels to create something new—an original product. Producing, generating, and planning are central to this cognitive process (Krathwohl, 2002).

In this course, students are given a few opportunities to create something new and original based on what they have learned. For example, each student designs, develops, and delivers a unique presentation on a cyber security topic of their choosing. They are given enough latitude so that they can be creative and have fun with the activity.

Another example is their team project. Students create a tri-fold brochure, develop a research paper, and some also created an informative and entertaining video.

Overall, the various types of activities in this course challenged students while keeping them engaged. Likewise, every cognitive process identified in Bloom's Taxonomy was used in multiple ways. Next, we discuss the results of two iterations of this course.

RESULTS OF TWO ITERATIONS

In this section, we discuss the results of two iterations of the course outlined herein. While no doubt there remains room for significant improvement, the initial results are promising. Part of the goal of the course was to expose students to information about cyber security that they did not previously know or understand. Based on some of the comments, this was accomplished:

- *"Helped me get more information about installing anti-virus software"*

- *"Should always have a backup"*
- *"I did not know much about computers so I learned a lot about them"*
- *"It opened my eyes to the dangers of the Internet"*
- *"It made me think of how unsafe I've been with my information online, but it also showed me what I could do to better protect myself"*
- *"Helped me understand the importance of cyber security"*
- *"It made me become more aware of my activities online and how I could protect myself by limiting what I post or do online*"
- *"I learned a lot more about computer safety and it made me think more about privacy"*
- *"I thought it was very relevant to everyday life"*
- *"The instructor made the material accessible and applicable to real life situations"*

Beyond exposure to new information on cyber security, we were interested in the efficacy of the approach taken. In particular, how effective were the lectures, videos, in-class activities, and labs? Below are some comments that address these questions:

- *"I enjoyed the labs as they pushed me to learn and analyze my own behavior in terms of digital security"*
- *"The class was very organized and slideshows that were presented by the instructor were easy to understand"*
- *"The hands on elements in the classroom and labs were great"*
- *"The lectures were very informational and helpful."*
- *"I also like the whole idea of applying terms/lessons learned in class to our real lives as assignments for the class"*
- *"I think the labs played an important role to make the material less theoretical and more hands on."*
- *"Practicing applications made the material more relevant and memorable"*

In addition to these comments, there was some constructive feedback that will be taken into account in future iterations. These comments are noted below:

- *"I was not a fan of the textbook"*
- *"The fact of being in a computer lab and having computers in front of me to easily distract me"*
- *"The room was very distracting. A lot of people were on Fb or online doing other stuff instead of listening"*
- *"I would suggest starting the lecture part in a classroom"*

When the course was created, a computer lab was requested. However, this turned out to provide too many distractions for some. It is unclear to what extent

this would be alleviated in a traditional classroom in which students may simply open their own laptops. Of course, the use of laptops in the classroom is something that can be addressed.

Additionally, as previously noted the text book for the course was suboptimal. There is a strong need for the development of a text book appropriate to teach cyber security to non-technical individuals. This does not mean that technical content should not be delivered as part of the curriculum; rather, it should be done in such a way that it is easily digestible by the non-technical person.

BENEFITS TO STAKEHOLDERS

Beyond the primary challenge of finding and/or developing an appropriate text book for this audience, there are also many benefits such a course provides to various stakeholders. For example, students learn how to better protect their information and improve their behavior from a cyber security and privacy standpoint. This is achieved through the numerous assignments and activities that have them directly engaging with their own computer systems and assessing their own cyber security and privacy behavior.

Divisions, departments, and schools also benefit by introducing an interesting topic in an approachable manner. Since cyber security and privacy touch on a variety of disciplines, this type of course has the potential to bring people into a variety of STEM and non-STEM majors. This can be particularly effective in bringing more women into the STEM majors since stereotype threat remains a very large impediment (Shapiro & Williams, 2012). Anecdotal evidence obtained through conversations with several of the female students suggests that this was the case as a few of them indicated they were now interested in computer science or information technology when they previously had not even considered it.

Colleges also benefit by providing an important class that serves as a public good while helping fulfill a general education requirement. Given the multi-disciplinary approach taken in this course, it has the ability to serve as an elective for different general education requirement categories, such as quantitative/symbolic reasoning, general science, philosophy/ethics, and/or social science. This benefits the student as they are generally able to fulfill a requirement needed for graduation, while also benefitting the college and its associated division, school, and/or department by providing an added incentive for the student to take such an important course.

Finally, society at large benefits by having more people educated in cyber security and privacy. These people are less likely to pose problems for organizations as non-malicious insiders, which present a security challenge due to curiosity, ignorance, and/or a lack of training and education (Ifinedo, 2012; Vance,

Siponen, & Pahnila, 2012). Likewise, they are also less likely to have their computers serve as botnets that can be used to target any number of corporate, financial, governmental, or military targets (Wash, 2010). Thus, having a course such as this is but one step that can be taken to make us all more secure.

DISCUSSION AND CONCLUSION

In this paper, we discussed the need for and development of an introductory cyber security course. The course was designed to introduce various cyber security and privacy topics to non-technical majors. While the focus has traditionally been on curriculum development for cyber security professionals, there has been increasing recognition that we also need to educate everyone else (Kam & Katerattanakul, 2014; Kritzinger & von Solms, 2010; Pfleeger & Caputo, 2012; Sobiesk et al., 2015). Thus, our goal here was to continue down this path in order to increase security for everyone.

Our approach included several different assessments and activities for the students with each cognitive processing level noted in Bloom's Taxonomy addressed in multiple ways. While the course was successful in two iterations thus far, there were some challenges. First and foremost, an appropriate text book for the intended audience needs to be developed. This is a difficult challenge to overcome given the time commitment needed for such an endeavor. In the meantime, it is possible courseware for the Certified Secure Computer User certification can be used or perhaps a custom eBook, which was done in our case.

Looking ahead, we plan to continue to make adjustments to the course, refine the curriculum, and improve the lab assignments. The hope is that through collaboration and continuous improvement, such a course can be developed that is sustainable and effective for college students throughout the United States and beyond.

REFERENCES

Baumann, K. A. (2016). *Computer Security in Elementary Schools: Faculty Perception of Curriculum Adequacy*. NORTHCENTRAL UNIVERSITY.

Bloom, B. S. (1956). Taxonomy of Educational Objectives, Handbook I: Cognitive Domain. *New York: David McKay*, *19*(56).

Case, R. (2013). The Unfortunate Consequences of Bloom's Taxonomy. *Social Education*, *77*(4), 196–200.

Certified Secure Computer User | EC-Council. (n.d.). Retrieved June 9, 2016, from https://www.eccouncil.org/Certification/certified-secure-computer-user

Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, *30*(8), 719–731.

Creeger, M. (2010). CTO Roundtable: Malware Defense. *Commun. ACM*, *53*(4), 43–49. https://doi.org/http://doi.acm.org/10.1145/1721654.1721670

Eydie, A. M. (2015). *How to be Anonymous Online: Step-by-Step Anonymity with Tor, Tails, Bitcoin and Writeprints*.

Frincke, D., & Bishop, M. (2004). Joining the security education community. *IEEE Security & Privacy*, (5), 61–63.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007

Ioannou, N. (2014). *Internet Security Fundamentals: Practical Steps To Increase Your Online Security* (06–2016 edition ed.). Boolean Logical Ltd.

Kam, H.-J., & Katerattanakul, P. (2014). Diversifying cybersecurity education: A non-technical approach to technical studies. In *Frontiers in Education Conference (FIE), 2014 IEEE* (pp. 1–4). IEEE.

Kessler, G. C., & Ramsay, J. (2013). Paradigms for cybersecurity education in a homeland security program. *Journal of Homeland Security Education*, *2*, 35.

Krathwohl, D. R. (2002). A revision of Bloom's taxonomy: An overview. *Theory into Practice*, *41*(4), 212–218.

Krathwohl, D. R., & Anderson, L. W. (2010). Merlin C. Wittrock and the revision of Bloom's Taxonomy. *Educational Psychologist*, *45*(1), 64–65.

Kritzinger, E., & von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security*, *29*(8), 840–847.

Leanage, H. (2012). *A Personal Internet Security Handbook* (3rd ed.).

Locasto, M. E., Ghosh, A. K., Jajodia, S., & Stavrou, A. (2011). The ephemeral legion: producing an expert cyber-security work force from thin air. *Communications of the ACM*, *54*(1), 129–131.

Locasto, M., & Sinclair, S. (2009). An Experience Report on Undergraduate Cyber-Security Education and Outreach. In *Proceedings of the 2nd Annual Conference on Education in Information Security (ACEIS 2009), Ames, IA, USA*.

Mann, M. I. (2012). People, Your Weakest Link. In *Hacking the human: social engineering techniques and security countermeasures* (pp. 39–61). Gower Publishing, Ltd.

Namin, A. S., Hewett, R., & Inan, F. A. (2015). Faculty Development Programs on Cybersecurity for Community Colleges: An Experience and Lessons Learned Report from a Two-Year Education Project. In *International Conference on Computer Science Education Innovation & Technology (CSEIT). Proceedings* (p. 19). Global Science and Technology Forum.

Omega, A. (2014). *The Best Book About Computer Security for Individuals, Families, and Small Business Owners* (2 edition). AmigOmega Publishing.

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security*, *31*(4), 597–611.

Pfleeger, S. L., Sasse, M. A., & Furnham, A. (2014). From Weakest Link to Security Hero: Transforming Staff Security Behavior. *Journal of Homeland Security and Emergency Management*, *11*(4), 489–510.

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the `weakest link'-a human/computer interaction approach to usable and effective security. *BT Technology Journal*, *19*(3), 122–31.

Schneider, F. B. (2013). Cybersecurity education in universities. *IEEE Security & Privacy*, (4), 3–4.

Shapiro, J. R., & Williams, A. M. (2012). The role of stereotype threats in undermining girls' and women's performance and interest in STEM fields. *Sex Roles*, *66*(3–4), 175–183.

Sobiesk, E., Blair, J., Conti, G., Lanham, M., & Taylor, H. (2015). Cyber Education: A Multi-Level, Multi-Discipline Approach. In *Proceedings of the 16th Annual Conference on Information Technology Education* (pp. 43–47). ACM.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management*, *49*(3–4), 190–198. https://doi.org/10.1016/j.im.2012.04.002

Wash, R. (2010). Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (p. 11). ACM.

Wineburg, S., & Schneider, J. (2009). Was Bloom's Taxonomy Pointed in the Wrong Direction? *The Phi Delta Kappan*, *91*(4), 56–61.

Young, J. B. (2008). Top 10 Threats to Computer Systems Include Professors and Students. *The Chronicle of Higher Education*, *55*(17), A9.