The Cyber Security Fair: An Effective Method For Training Users To Improve Their Cyber Security Behaviors?

Stephen Larson
School of Business
Slippery Rock University of PA
stephen.larson@sru.edu

ABSTRACT: *The effort to raise cyber security awareness is widespread and growing. At our small liberal arts university, we held a cyber security fair, with the topics presented by students to students. This paper describes our experience and our effort to determine whether a cyber security fair is an appropriate venue for raising awareness of cyber security issues and to train users to improve their cyber security behaviors.*

Keywords: Cyber Security, Training, Security Awareness, Service Learning

Received: 22 December 2014, Revised 28 January 2014, Accepted 3 February 2015

1. Introduction

The need to increase the cyber security awareness level of end-users continues to be broadcast in the media. To help fill the need, there are numerous websites that offer free training – for example, the Center for Internet Security lists several organizations that offer free training and webcasts for cyber security awareness (Center for Internet Security, 2013), a global cybersecurity awareness campaign called Stop.Think.Connect™, led by the National Cyber Security Alliance (NCSA) and the Anti-Phishing Working Group (APWG), contains a cornucopia of campaigns, research, and resources aimed at helping increase the awareness of cyber security and improve America's cyber security level (Stop.Think.Connect. (2013). Naturally, the US government is a stakeholder and major supporter; in 2010 President Obama proclaimed October to be National Cyber Security Awareness Month and called upon "upon the people of the United States to recognize the importance of cybersecurity" (Obama, 2010).

As expected, government agencies are well aware of the need for cybersecurity training. Macmanus, et al. stated "More funding, personnel, equipment, and training, better software, more rigorous enforcement, and clearer standards and procedures are needed to balance privacy protection and transparency in cybersecurity policy making." (Macmanus, Caruson, & McPhee, 2013). McDaniel stated the need for a comprehensive strategy for education, training, and awareness of the U.S. Department of Defense workforce - military, civilians, and contractors (McDaniel, 2013).

Numerous experts also agree there is a need for end user training in cyber security; we will mention but a few. Jerry Johnson, chief information officer of U.S.-based Pacific Northwest National Laboratory (PNNL), a US government think tank, says he is amazed at the level of insecurity that persists at many organizations and that the most critical defense against cyber attack is end-user training (Preston, 2007). Major General Ronnie D. Hawkins, Jr. stated "Every network user must be educated and trained about Internet security" (Beidel, 2011). Bradley Peniston, editor of the Armed Forces Journal, agrees that "cybersecurity or network security begins

with user training" (Peniston, 2013). Additionally, simple, yet effective, training must be provided to personnel for general awareness, for as long as there are cyber criminals ready to strike, companies remain vulnerable. CEOs and government officials were admonished that "Cyber-security training and education must be your company's top priority" (VanDerwerken&Ubell, 2011).

As there is a need to teach cyber security awareness, we endeavored to provide a learning opportunity to the most students possible without requiring attendance of a course or a formal workshop. We also wanted to discover if learning about good cyber security behaviors would be possible in a fair-like setting.

2. Current Cyber Security Offerings

While the need for end-user training is clear, the best way to train end users is unclear. Only a few states have established curricula for teaching students to deal with cyber bullying, identity theft and online predators, and a majority of teachers feel they have received insufficient cyber security training to teach cyber security to their students (Miners, 2009). A study by the National Cyber Security Alliance (NCSA) and sponsored by Microsoft Corp. stated that 55 percent of educators strongly agree that cyberethics, cyber safety and cyber security should be learned in schools. However, K-12 schools in the USA are not ready to teach the fundamentals of online safety, ethics and security (Computer Security Update, 2011). Hence, current college students may not have learned the fundamentals of online safety, ethics and security.

The offerings by colleges and universities seem to be quite plentiful. Higher education institutions offer cyber security training that includes everything from tweets and blogs, graphic posters, website banners, and news announcements to full courses, and in some cases undergraduate and graduate degrees in cyber security. The National Cyber Security Awareness Month (NCSAM) campaign lists over 190 cyber security awareness events that were held during October 2013 (Higher Education Information Security Council, 2013).

One example is Virginia Commonwealth University's cyber security fair, which

"promotes a secure culture with in VCU and is designed to provide information-security education and training to all constituents within the VCU community. Attendees learn about the ways to protect their personal information from cybercriminals, as well as ways to secure their electronic devices at home and work. Technology vendors are on site to demonstrate the latest and greatest technology, and IT support staff answer technology- and security-related questions" (VCU, 2013).

VCU's cyber security fair brings in speakers to educate attendees about cyber security topics, as well as informational booths, some with prizes. Similar activities can be seen in numerous cyber security fairs throughout the higher education offerings.

Another university that holds an annual cyber security fair is California State Polytechnic University, Pomona, which will have its tenth fair in October 2014. Cal Poly Pomona's fair includes presentations from industry leaders, peer to peer demonstrations, vendor exhibits, activities and door prizes. The main purposes of this fair is to advance and support information technology security awareness, provide hands on peer to peer mentoring with security concepts, and teach users how to protect data from intentional or accidental loss through the deployment of common security practices.

3. Our Cyber Security Fair

Our university is a small, rural university in the northeastern USA with a student population of just over 8,000. 91% of the students are undergraduates; and 93% of undergraduate students are full time students. The average number of students per class level is around 1,600, with the exception of freshmen at around 2,000 students. Demographically, the student body is 58% female and 42% male. 88% of the students are in-state, with 11% out of state and 1% international. 86% of the student body is between the ages of 18 and 24, 1% are 17 and under, 7% are aged 25 – 29, and 6% are above the age of 30.

There were three goals for our cyber security fair: 1) to give students an opportunity for service learning, 2) to evaluate the cybersecurity awareness levels of our student population, and 3) to determine whether a cyber security fair is an appropriate venue for teaching good cyber security behaviors.

Students in a junior-level liberal studies/general education cyber security course were asked to teach what they had learned in the

course to other students in the form of a cyber security fair. The students were divided into teams, with each team tasked to become subject matter experts on a particular cyber security behavior, and subsequently teach fellow students.

Our cyber security fair consisted of several booths, all of which taught various good cyber security behaviors.The topics and behaviors taught at each booth was designed to take less than 5 minutes. The fair was designed to take less than an hour to visit so attendees could fit a visit in during the long lunch hour and common hour during which there are no classes. The booths, manned by students, included:

• Gone Phishing – attendees will fish and catch an email message, which they then will have to determine whether it is a phishing message or a legitimate message. Participants will learn how to recognize phishing email messages and what to do when they receive one.

• Don't Forget to Wipe – attendees will learn how to securely delete all data on a hard disk before disposing of a computer, a process called "wiping" the hard disk.

• Smart Phones, Stupid People – attendees will learn how to secure their smart phones to not give out data unintentionally, and how to encrypt and password protect their data.

• Social Media – attendees will learn the perils of using social media, and how to protect their personal information on social networking sites.

• P@ssW0rd – attendees will learn what constitutes a strong password, and have an opportunity to test the strength of their password(s).

• Are You Backed Up? – attendees will learn the proper way to back up their critical data and test the restoration of backed up data.

• Are You Using Protection? – attendees will learn how to protect their data with encryption.

• Safely Using Public PCs and Wifi Hotspots – participants will learn how to safely use public PCs and Wifi hotspots, which activities are safe to do and which are not.

• Viruses and Malware – attendees learned about various viruses and malware, and how to protect against them. Various anti-virus software packages are explained, as well as how to configure the software for auto-update and scanning.

Our cyber security fair was set up so that attendees visited a "registration" desk at which they completed a pre-quiz and received an attendance card. As the participants visited each booth, the booth attendant would stamp their card. To ensure the attendees learned all the information necessary to successfully complete the post-quiz, attendees had to visit all the booths and get their card stamped to be entered for the prize drawing. Door prizes included the grand prize of a Dell© laptop and a first prize of a tablet PC; other prizes were gift cards for local merchants, free copies of encryption software, USB memory sticks, etc.

PR and advertising for the fair was managed by a student PR group. They designed posters and fliers, and put them up in the residence halls and classroom buildings. Additionally, table tents were placed on all tables in the student dining facilities. The on campus newspaper ran an article the week before the fair and the student center where the fair was held also had posters and advertisements on its large screen monitors. On the day of the fair, lawn signs were placed in high foot traffic areas to direct students to the fair.

4. Assessing the Cyber Security Fair Method

Unfortunately, we were unable to find a cyber security fair that measured whether attendees learned good cyber security behaviors through attendance. Most of the fairs had booths that taught good cyber security behaviors, such as what constitutes a strong password, how to recognize a phishing email message, how to encrypt data, and so forth. Some even had a quiz attendees could take at selected booths. At our institution we wanted to raise cyber security awareness among the university community, but we also believe that we needed to assess the training we will do to ensure this is an effective method of raising cyber security awareness.

The students in a liberal studies course on cyber security taught cyber security behaviors at the booths and developed a quiz on cyber security to evaluate the participants' knowledge of good cyber security behaviors (see the Appendix). The students collaborated on the quiz questions to ensure everyone agreed that these questions would measure the cyber security awareness level they believed college students should have. This quiz was given to attendees before entering the cyber security fair. The quiz was administered via scantron sheets. After visiting all the booths, the participants took the same quiz as a post-test. To ensure we could compare the participants' pre- and post-test answers anonymously, the post-test answers were on the back side of the pre-test scantron sheet. This also helped eliminate bias as it discouraged looking at the pre-quiz answers by requiring the participant to flip the paper over and back again to view the pre-quiz answers.

5. Discussion and Conclusion

5.1 Analysis of Pre- and Post-Test Results

The pre- and post-tests were the instruments used to measure two of the three goals of the fair. The results of the pre-test were used to measure the cyber security awareness level of the student population. The post-test results were used to measure whether a cyber security fair is an effective method to teach good cyber security behaviors.

Given that there was no evidence found in the literature that a cyber security fair is an effective method of teaching cyber security behaviors, we hypothesized that there will be no difference between the average scores on the pre-test and post-test (H0 = 0). A t-test was performed to compare the average scores on the pre-test and post-test. The results are shown in Table 1.

The average score on the pre-test (21 questions, $N = 90$) was 17.42 out of 21, or 83%. The highest score was 100%, the lowest score was 5 (24%) with a mode of 19 (90%). These pre-test scores show that the student population that attended the fair performed fairly well on the pre-test, suggesting that the student population is versed in good cyber security behaviors, and have a fairly high awareness of cyber security issues. This was unexpected given our rural location. Our goal of assessing the cyber security awareness level of our students was accomplished.

The average score on the post-test was 17.55 out of 21, or 84% ($N = 64$), the highest score was 100%, the lowest score was 9 (43%), and the mode was 18 (86%). There were 26 questionnaires that did not have the post-test completed and several others that were incomplete. These questionnaires were discarded and not used in the study.

In our study, the differences in the means were not statistically significant. The mean score on the pre-test was 17.42, while the mean score on the post-test was 17.55. The p value is .728. The statistical analysis results are not convincing enough to say that the mean scores on the pre-test and post-test differ significantly, and we fail to reject the null hypothesis that there is no difference in the means. Therefore, we conclude that for most participants, learning did not occur through attending the cyber security fair, and that raising the awareness level of good cyber security behaviors did not occur. Our goal of determining whether a cyber security fair is an appropriate venue for teaching good cyber security behaviors was accomplished.

5.2 Student Feedback

Feedback from the students in the cyber security course who taught at the fair implied that they not only enjoyed the opportunity to teach, but they also learned new information and practiced critical thinking skills. Through their comments and those of a few participants, we concluded that the goal of giving the students a service-learning experience was accomplished. Comments included:

"I learned more about smart phone security through teaching it than I did in class."

"It was fun to teach fellow students."

"I was asked questions I had never thought of while preparing to teach about safe social networking."

"Many of the attendees seemed to be more knowledgeable than I on encryption. I think it is because they are computer science or IT majors."

"Where did you find all these professionals to present and teach here?" (from a non-student attendee)

"This looks like fun – I want to do it when I take this class" (from a student attendee)

We also had a student asking the attendees a trick question. For a prize of a USB drive, participants who were finished filling out

the post-test were asked to give is their network login ID, which also serves as their university email address. Having just learned that one should not give out a login ID, several students commented that they thought this was a trick question – they wanted to win the USB drive, but they were reluctant to give their network login to another student. (Naturally, those students won a USB drive.)

6. Lessons Learned

As with all first-time projects, we learned several lessons; some were expected and some were not. Though there are quite a few lessons learned; we will mention but a few:

• Have a quicker way for students to fill out the pre-test. Due to our set up, we had only three six-foot long tables at which attendees could take the pre-test. This created a long line (at times over 50 people) of people waiting to get into the fair. Having a speedier way to take the pre-test would allow more students the opportunity to attend the fair. Several attendeesdid not take the post-test as they ran out of time and had to go to class. There were more participants who did not take either test than who took the tests due to time constraints.

• Additionally, have separate answer sheets for the pre- and post-tests. Though an ID number would have to be created and printed on both sheets, this would alleviate some confusion as to which side of the answer sheet was to be filled in for the pre- or post-test.

• Separate the booths more. The booths (tables) were quite close together, and it was difficult for the participants to concentrate on each individual booth without getting distracted by the next booth.

• Put the Wifi booth far away from the password booth. At the password booth, participants learned about strong passwords, and then typed a password on a website which tested the strength of the password. The computer on which this occurred was connected wirelessly to the internet. At the Wifi booth, in addition to learning about HTTP versus HTTPS and what kinds of activities are safe to do on a public Wifi hotspot, attendees saw what kind of information could be captured by packet-capturing software (Wireshark©) that was capturing wireless traffic. Though the password website was connected via HTTPS, many participants were hesitant to enter their password for fear it could be captured.

• Have separate booths for iPhones, Android phones, and Windows phones. Teaching about all of these at one booth was confusing for some participants.

• Arrange the booths in the order which we want participants to visit them. Most of the students followed the order the booths were arranged, though some booths presented material that depended on information that was to be learned previously at another booth. Arranging booths in the order in which we wanted information presented would mitigate the issue. For example, we should have the students visit the password booth before visiting the WiFi booth.

• Hold the fair later in the spring or early in the fall so snow does not keep participants away.

• Set a date and keep to it. Local vendors and sponsors planned to have booths at the fair, such as the local bank (where many students have accounts) and the local internet provider. The bank intended to provide information on how they keep the students' information and online banking safe; the local internet provider also intended to provide information on how their system keeps students safe online. Yet the university administration changed the date of the fair and both these important sponsor/vendors canceled.

7. Future Research

As this was our first cyber security fair, we found some information that we would like to gather and analyze in our next fair. For example, we would like to ensure that participants fill out the demographic questions on the pre-test so that we may analyze the differences between gender, age, class level, and the majors of participants who attended the fair and took the pre- and post-tests. We suspect that the average scores were high due to many of the participants being computer science, information systems, or information technology majors because several faculty in the Computer Science Department offered extra credit to their students for attending the fair.

We also plan to analyze each question type to find out whether certain topics were challenging for participants or whether topics could be only lightly touched upon. For example, what constitutes a strong password may be common knowledge, while encryption may be a challenging topic for our participants.

Finally, the test questions were developed by the students; we would like to ask our colleagues for feedback on our test questions to ensure we are asking appropriate and relevant questions.

T-Test Results		
	Post-test	**Pre-test**
Mean	17.55	17.42
Variance	3.87	6.04
Observations	64	90
Standard Deviation	1.97	2.46
Hypothesized Mean Difference	0	
df	150	
t Stat	0.349	
P(T<=t) one-tail	0.364	
t Critical one-tail	1.656	
P(T<=t) two-tail	0.728	
t Critical two-tail	1.976	

Table 1. T-test Results

We would also like to perform a more granular analysis of the results, including which questions on the pre- and post-tests were missed the most often, which questions were missed on both pre- and post-tests, which questions were answered correctly most often, and which questions were answered correctly on the pre-test but not the post-test.

8. References

[1] Beidel, E. (2011). Protectors of Critical Networks Look Within For Vulnerabilities, *National Defense*, 96 (693), p. 36.

[2] Center for Internet Security (2013). Cyber Security Awareness Free Training and Webcasts, Retrieved February 5, 2014, from *Multi-State Information Sharing and Analysis Center*: http://msisac.cisecurity.org/resources/videos/free-training.cfm

[3] Computer Security Update. (2011). U.S. Schools not preparing kids for digital age, *Computer Security Update*, 12 (6), p. 1-5.

[4] Higher Education Information Security Council. (2013). National Cyber Security Awareness Month Resource Kit, Retrieved February 5, 2014, from *Information Security Guide*: https://wiki.internet2.edu/confluence/display/itsg2/NCSAM+Resource+Kit

[5] Macmanus, S. A., Caruson, K., McPhee, B. D. (2013). Cybersecurity at the Local Government Level: Balancing Demands for Transparency and Privacy Rights, *Journal Of Urban Affairs*, 35 (4), 451-470.

[6] McDaniel, E. A. (2013). Securing the Information and Communications Technology Global Supply Chain from Exploitation: Developing a Strategy for Education, Training, and Awareness, *Issues In Informing Science & Information Technology* (10), p. 313-324.

[7] Miners, Z. (2009). Who's Keeping Students Safe Online? *District Administration*, 45 (1), 12.

[8] Obama, B. (2010). Presidential Proclamation—National Cybersecurity Awareness Month. Retrieved February 5, 2014, from the White House: http://www.whitehouse.gov/the-press-office/2010/10/01/presidential-proclamation-national-cybersecurity-

awareness-month.

[9] Peniston, B. (2013). Someone else's problem. *Armed Forces Journal*, 150 (9), p. 6.

[10] Preston, R. (2007). Pacific Lab Breathe Cybersecurity, *Information Week* (1157), p. 30.

[11]Stop.Think.Connect. (2013). About Us, Retrieved February 5, 2014, from Stop.Think.Connect: http://www.stopthinkconnect.org/about-us/overview/

[12] VanDerwerken, J., Ubell, R. (2011). Training on the Cyber Security Frontlines, *Training and Development*, 65 (6), p. 46-50.

[13] VCU(2013). Cyber Security Fair @ Tompkins-McCaw Library, Retrieved February 4, 2014, from Virginia Common wealth University: http://www.ts.vcu.edu/cybersecurity/

9. Author Biography

Dr. Stephen Larson is an assistant professor of Information Systems at Slippery Rock University of PA. Prior to entering academia, he spent nearly 20 years in the computer technology field, working on projects with several computer security companies, finance firms, and high tech firms, rising to the level of country manager before leaving industry for academia. He enjoys teaching and researching about computer security and forensics.

Appendix: Pre- and Post-Test Questions
The questions for the pre- and post-tests were the same, except for the final question (#22), which was added for the post-test.

1. Which of the following would NOT be included in a strong password?
a. Uppercase and lower case letters
b. Numbers
c. Special characters
d. Numbers or letters in sequence (e.g. 5678 or jklm).

2. All of these are backup devices except:
a. External hard disk drive
b. Cloud
c. USB memory stick
d. Computer's hard disk drive

3. Whose friend requests should you accept on a social networking site?
a. Friends of friends
b. Anyone who asks
c. Only people you personally know
d. Celebrities, famous, or rich people

4. You can encrypt cell phone data (T/F).

5. What are some signs that your computer may be infected with a virus or other malware
a. It is running slower than usual
b. Programs are opening or closing without permission
c. Programs appear that you did not install
d. All of the above

6. An email message from your mother can never be a phishing email (T/F).

7. Is free Wifi safe to use for online banking, shopping, or checking email? (Y/N)

8. What are ways of protecting your personal data?
a. Tell your friends your passwords so if you forget you can ask them

b. Encrypt your data
c. Keep a backup of your data
d. Both B and C

9. Which of the following passwords is the strongest?
a. The name of your pet, with numbers added (like Snowball3)
b. Passw0rd
c. Barny_Stinson
d. Willd0work4food!

10. How often should you back up your data?
a. Every day
b. As often as needed
c. Once a week
d. Once a month

11. How can you avoid being a victim of phishing within a social networking site?
a. Don't click on unknown links in someone's post
b. Don't give out your email address
c. Don't share other people's posts or re-tweet
d. Don't direct readers to your other social networking sites
e. All of the above

12. What security issues do cell phones have?
a. Viruses or other malware
b. Shoulder surfing
c. Lack of screen password or swipe pattern
d. All of the above
e. None of the above – my cell phone is secure

13. What is the first thing you should do if you think your computer is infected with a virus or other malware?
a. Smash it
b. Turn it off
c. Run a virus scan
d. Disconnect it from the internet

14. Which of the following is a valid, secure URL for Paypal?
a. http://www.paypal.orders.com
b. https://www.paypal.com
c. https://www.playpal.com
d. http://www.paylap.com

15. What can you safely do on a public PC?
a. Shopping
b. Online banking
c. Surf the web
d. Download files
e. Email

16. Which is best: a long password (14 or more characters), a complex password with letters, numbers, and special characters, or a long, complex password?
a. A long password
b. A complex password
c. A long, complex password

17. How can you best protect your personal information on a social media site?
a. Share your personal information only with friends and friends of friends
b. Share whatever information you are comfortable sharing
c. Keep all information, pictures, friends, etc. private
d. Just use the social media's default privacy settings – they are there to protect the users.

18. Screen locking passwords or swipe patterns are sufficient to protect a cellphone (T/F).

19. What is a good way to tell if a website can be trusted before downloading any files or entering personal information?
a. Look for it on Wikipedia
b. There is no way, just take your chances
c. Look for the lock icon in the address bar or the "s" after http
d. None of the above

20. What is the goal of a phishing attack?
a. To capture the user's keystrokes?
b. To trick the user into giving away personal information
c. To duplicate legitimate services
d. To catch fish

21. When logging into a website when using a public or shared PC, should you check the "remember me" box?
a. Yes
b. No

The last question was added for the post-test only:

22. If there is a class on practical computer security that filled a Liberal Studies requirement, would you be interested in taking the class?
a. Yes
b. No