Emily Vandalovsky

Project 1 – Quantitative Study

EDTC 806 – Research Methods

Spring 2018

Dr. Carnahan

Chapter 1 - Introduction

As cyber attacks increase in frequency, complexity, and severity around the globe, the need for a general cybersecurity awareness becomes essential. The threat of unauthorized data access and leaking sensitive information is real and frequent occurrence (Robinson, Brown, & Green, 2010, pp. 56-58). The viable and sustainable mechanisms are needed to withstand the existing threat.

With various areas of vulnerability apparent in cyberspace, the human element continues to be considered one of the most critical components in cyber exploits and data leaks (Champion, Jariwala, Ward & Cooke, 2014). The internal threats exist as a "result of poor user security behavior", according to Goodwin (2005). The protection of cyberspace can no longer be the prerogative of a group of professionals, regardless of highly trained they are. For cybersecurity awareness to become every user's personal and civil responsibility (McGettrick, Cassel, Dark, Hawthorne & Impagliazzo, 2014), the end-user mentality has to change (Robinson, Brown, & Green, 2010, pp. 66). From the public awareness perspective, the cybersecurity if similar to public health (Mulligan & Schneider, 2011), when technology users have to understand and exhibit digital health norms. Public digital hygiene is a strong mechanism against malicious behaviors (Paulsen, McDuffie, Newhouse & Toth, 2012).

One of the commonly stated challenges of cybersecurity awareness and education lays within the definition of the field. The term cybersecurity implies the very act of securing or protecting cyberspace from unauthorized use. For the purposes of this paper, it is helpful to think of cyberspace as not only the Internet's infrastructure of networked computers, routers, fiber-optic cables, cellular technologies and traveling data, but also as people involved in implementing these processes and the decisions they make.

In their book Cybersecurity: what everyone needs to know, Singer & Friedman state: “cyberspace is defined as much by the cognitive realm as by the physical and digital. Perceptions matter and they inform cyberspace’s internal structures in everything from how the names within cyberspace are assigned to who owns which parts of the infrastructure that powers and uses it.” (Singer & Friedman, 2014, p.14).

This paper studies the perception of cybersecurity awareness and its realization in the online behavior. As the overall rate of cybersecurity threats continues to grow, so is the number of cyber attacks on colleges and universities **(citation.- ???).** The community of college computer users, including but not limited to faculty, students and staff members, exhibit certain online behaviors that contribute to the overall safety of college's computing environment. Since the human factor continues to be the leading cause of cybersecurity attacks (Champion, Jariwala, Ward & Cooke, 2014), all college computer users have a responsibility of protecting their commonly shared cyberspace. This study will focus on the student population and their role in preventing cyber attacks by exhibiting safe online behaviors. Other groups of computer users including but limited to faculty and staff, will remain outside the scope of this study.

The current college students are considered digital natives who freely navigate through cyberspace and operate within boundaries of many networks (Muhirwe & White, 2016). The main purpose of this study is to investigate the status of cybersecurity behaviors for the currently enrolled students at a Community College in northeastern United States. The goal of this study is to examine the differences between perception and implementation of cybersecurity-aware practices and to investigate whether an increase in awareness and training have any significant impact on students’ cybersecurity minded behaviors.

To investigate the extent of the safe behavior of students in the cyberspace, the following research questions will be approached:

Question 1: to which extent are students aware of cybersecurity-related practices?

Question 2: to which extent do students practice the cybersecurity-related tasks?

Question 3: does the completion of cybersecurity training have any significant impact on the student's awareness of cybersecurity?

Question 4: does the completion of cybersecurity training have any significant impact on the student's cybersecurity-related practices?

Chapter 2 – Literature Review

The topic of cybersecurity is largely extensive and has served as an area of interest for many researchers for a number of years. A combined search for "cybersecurity" or "cyber security" (which is used both ways by some authors) using Google Scholar database alone returns over two hundred thousand entries. The number of publications greatly decreases when the focus narrows into the cybersecurity awareness. Multiple searches among several databases on the topic of cybersecurity awareness among college students produce limited results, with the extremely low number of studies performed in the community college setting.

The lack of sufficient published editions on the topic of the cybersecurity awareness among community college students identifies the gap in the existing literature and allows for the further investigation and research on the topic.

The existing literature on cybersecurity awareness in the college setting could be attributed to two categories. The first category of publications focuses on perception and use of cybersecurity practices exhibited by the college students (Lomo-David & Shannon, 2009; Teer, Kruck & Kruck, 20007). The focus of the second category relates to the cybersecurity awareness training and the cognitive behaviors associated with it (Kim & Homan, 2012; Scheponik et al., 2016; Tyworth et al., 2012; Jansson von Solms, 2013; Stark, 2017). The current study incorporates elements of both categories and extends the research in both areas.

In their study, Lomo-David & Shannon (2009) investigated the differences between the knowledge of information system security safety measures and the actual use of them on a daily basis. Based on the survey received from 867 students, Lomo-David & Shannon established that in six out of ten cases, the familiarly with (or knowledge of) the information system security safety measures had a direct impact on their usage. The research called for the further need to educate students on safe cyber behaviors using supplemental methods (Lomo-David & Shannon, 2009).

The study included a 24-question survey that was randomly distributed to 20 out of 90 universities in Nigeria. The survey included questions on familiarity and usability of the following information system security measures: simple passwords, sophisticated passwords, and daily computer system scan, the scan of email attachments, anti-virus software, and password on email attachments, biometric authentication, firewalls, intrusion detection systems and multifaceted authentication systems. The researchers hypothesized on the lack of the significant relationships between the familiarity with any of the above-listed safety measures and their usage (Lomo-David & Shannon, 2009). The investigation established that in six cases out of ten there was a significant relationship established between the familiarity and the use of the above-mentioned measures.

There were several limitations to the study. In addition to being criticized by other researchers for the redundancy, ambiguity, and readability of questions (Lomo-David & Shannon, 2009), the instrument wasn't clear. t was not stated in the publication whether the questions were related to home or college computers, and in case of the latter one, whether or not the respondents were involved in some way in monitoring or protecting college's computer system. The research confirmed the existence of the significant relationship between the knowledge and the use of such security measures as firewalls, anti-virus software, scanning emails for viruses and daily computer scans. However, these measures do not require any input from the individual users and are automatically setup by the system. This provides a limitation to the viability of the research.

In the similar study, Teer, Kruck & Kruck performed empirical research and documented computer security practices and perceptions among undergraduate students (2007). The study surveyed one hundred students from Computer Information Systems, Art and Integrated Science and Technology programs on the use and perception of such computer security measures are antivirus programs, firewalls, opening attachments, passwords and security patches (Teer, Kruck & Kruck, 2007).

Eighty-six out of one hundred undergraduate students from one large four-year public state university on the east coast returned the survey. Thirty-seven percent or responders were CIS majors, twenty-nine were Integrated Science and Technology majors, and thirty-four percent were Art majors. Fifty percent of responders were seniors. The questions specifically attributed to the safety measures taken by the students on campus as well as their personal computing devices (Teer, Kruck & Kruck, 2007).

The results were categorized by major and by the type of online security behavior. In addition, participants conveyed their perception of the importance of computer security. Numerous occurrences of unsafe cybersecurity practices were reported in this study, indicating the prevalence of unsafe computing behaviors and increased vulnerability cybersecurity threats. Seven percent of the participants stating that their home computers were "very insecure" and twenty-two percent stating that their home computers were "very secure". The majority of responders indicated that their home computers were "somewhat insecure" (Teer, Kruck & Kruck, 2007).

This study concluded that majority of students reporting their home computers on the "insecure" part of the scale. At least a half of respondents considering it important for their home computers to be secure, so there could be a "general lack of knowledge among the students on both the need for home computer security and how to better protect their home computers" (Teer, Kruck & Kruck, 2007, p.109).

While this study appears viable and effective, the following limitations may seem apparent. The responses received from the study participants represented their perceptions of the situation, and not verifiably valid answers. Since only students from three different majors were surveyed, a non-response bias may have taken place. There may not be enough evidence for generalizing results to other majors or universities (Teer, Kruck & Kruck, 2007).

In their qualitative study, Scheponik et al., focus on reasoning about core cybersecurity concepts (2016). The study was conducted at the three diverse institutions, including one community college, which in itself is already an isolated occurrence. In addition, the researchers claim for this study to be the first one to explore the student cognition and reasoning about cybersecurity. The study is effective in the way it deals with the research questions on presenting a broad range of way that students are challenged to reason using adversarial mentality and misinterpret cybersecurity concepts (Scheponik et al., 2016). With its focus on specific scenarios and the student reasoning associated with them, this type of studies is an important complement to quantitative studies on the related topic.

In the study on the distributed nature of cyber situation awareness, Tyworth, Giacobe, Mancuso & Dancy implement a slightly different approach, known as the living lab approach (2012). This concept of the living lab incorporates theory and practice in a never-ending cyclical model allows for viewing the cybersecurity awareness from a different angle. This qualitative study was comprised of twenty-three interviews with cybersecurity professionals and the ethnographic observation of cadets from the United States Military Academy (Tyworth et al., 2012).

Included in the category of the cybersecurity behavior related studies, there is a published experiment of cultivating user's resistance towards phishing attacks upon completion of the training (Jansson & von Solms, 2013).

3. Methodology

There is an ever-growing need for promoting cybersecurity by understanding and adapting safe online practices. With its multifaceted environments, cybersecurity could be attributed to a number of online safety measures, some of which are automatically performed and managed by the professional staff at the college. However, it remains students' responsibility to setup and maintain cybersecurity-mindful practices while using their own computing equipment.

For this study, the data is collected on certain cybersecurity awareness practices using online survey mechanism from students enrolled in Introduction to college experience course at the community college in the northeastern United States. Using simple random sampling, the survey is distributed to ten random sections of the course, with the total number of two hundred students enrolled. Since the Introduction to College experience course is offered to students of all majors, the make-up of majors and programs of study represented in this survey sample will be unknown to the researcher until the time of the experiment. This should limit some of the researcher-related bias in the pre-selection of majors.

At the beginning of the semester, the students will be presented with a twenty-question survey on their existing practices relating to cybersecurity. The questions will focus on the following two areas: the awareness of cybersecurity minded behaviors and the application (the usage) of that knowledge on the regular basis. The answers to these questions will be recorded as a pre-intervention result set. Ten questions on the survey are geared towards cybersecurity awareness, and ten other questions, marked with a (*) on the survey focus on the cybersecurity practices. The survey is presented in Appendix A.

Within a week of conducting the original survey, the students will be presented with a set of activities and exercises on the topics of importance of cybersecurity awareness. Students will be offered to complete hands-on exercises and discuss real-life examples. This kind of training will provide an intervention treatment and allow all students to practice cybersecurity minded behavior in a classroom setting.

In a week of completing the intervention training, the students will be offered to repeat the survey. The answers to these questions will be recorded as the first post-intervention result set. It will assist with answering the following research question: does completion cybersecurity training have any significant impact on the student's awareness of cybersecurity?

To recognize the differences between the awareness of and applicability (the usage) of cybersecurity-related behaviors, the same survey will be distributed once again to the same group of students within 30-60 days period after completing the last one. One to two months span between the training and the last survey will allow students to establish the raised awareness and reinforce it into practice. Completing the last version of the survey will assist with answering the following research question: does completion cybersecurity training have any significant impact on the student's cybersecurity-related practices?

In addition to collecting pre- and post-training figures, the following demographic data will be collected: age, gender, the number of credits completed, declared major or program of study, the number of computing devices owned and name as an optional entry. In this study, the independent variable is represented by the conducted training; the dependent variables are represented by the short-term awareness and practice survey (7-day) and the long-term awareness and practice survey (30-60 day). Demographic data provides additional information further data analysis.

During the data collection process, the answers to questions 1 – 20 will be assigned numeric values as follows:

__ (5) yes
__ (4) to a great extent
__ (3) to some extent
__ (2) to a small extent
__ (1) no.

In comparing the results of the pre-training survey with the first post-training survey, conducted in a 7-day period, the questions numbered 1, 2, 4, 6, 8, 11, 13, 16, 18 and 20 will contribute the data points to test the following null hypothesis:

> H_0: there is no significant difference in the participants' perception of the knowledge level in cybersecurity awareness before and after the training.

In comparing the results of the pre-training survey with the second post-training survey, conducted within 30-60 day period, the questions numbered 3, 5, 7, 9 10, 12 14, 15, 17 and 19 will contribute the data points to test the following null hypothesis:

> H_0: there is no significant difference in cybersecurity-related practices exhibited by participants before and after the training.

Conducting this experiment in a two-fold manner, described above, allows the researcher to employ a variety of statistical and analytical tools for performing data comparisons and drawing conclusions.

Appendix A

Student Cybersecurity Awareness and Practice Survey

1. Do you agree that Cybersecurity Awareness and Practice should not be limited to professionals who administer and support computing devices?
__ yes __ to a great extent __ to some extent __to a small extent __no

2. Are you familiar with the term personally identifiable information (PII)?
__ yes __ to a great extent __ to some extent __to a small extent __no

3. (*) Are you involved in practices protecting personally identifiable information (PII)?
__ yes __ to a great extent __ to some extent __to a small extent __no

4. Are you familiar with the concept of social engineering?
__ yes __ to a great extent __ to some extent __to a small extent __no

5. (*) Are you involved in practices protecting against social engineering?
__ yes __ to a great extent __ to some extent __to a small extent __no

6. Do you consider yourself knowledgeable about identifying malicious attacks sent via email attachments?
__ yes __ to a great extent __ to some extent __to a small extent __no

7. (*) If you received a suspicious email would you know how to deal with it?
__ yes __ to a great extent __ to some extent __to a small extent __no

8. Do you consider yourself knowledgeable about identifying phishing attacks?
__ yes __ to a great extent __ to some extent __to a small extent __no

9. (*) Are you involved in practices protecting against phishing attacks?
__ yes __ to a great extent __ to some extent __to a small extent __no

10. (*) Do you scan received email attachments?
__ yes __ to a great extent __ to some extent __to a small extent __no

11. Do you consider yourself knowledgeable about identifying and protecting against malicious links and websites?
__ yes __ to a great extent __ to some extent __to a small extent __no

12. (*) Do you practice identifying and reporting illegitimate websites or links?
__ yes __ to a great extent __ to some extent __to a small extent __no

13. Do you consider yourself knowledgeable about best practices in cybersecurity?
__ yes __ to a great extent __ to some extent __to a small extent __no

14. (*) If your home computer system became infected with a virus, would you know how to deal with it?
__ yes __ to a great extent __ to some extent __to a small extent __no

15. (*) Do you find system security patches annoying and unnecessary?
__ yes __ to a great extent __ to some extent __to a small extent __no

16. Do you consider yourself knowledgeable about creating strong passwords?
__ yes __ to a great extent __ to some extent __to a small extent __no

17. (*) Do you use strong passwords even when the authentication mechanism does not enforce it?
__ yes __ to a great extent __ to some extent __to a small extent __no

Student Cybersecurity Awareness and Practice Survey

18. Do you consider yourself knowledgeable about reporting a potential breach or attack?
__ yes __ to a great extent __ to some extent __to a small extent __no

19. (*) Do you log off or turn off your computer when you leave?
__ yes __ to a great extent __ to some extent __to a small extent __no

20. Do you consider yourself knowledgeable about cybersecurity threats in mobile devices?
__ yes __ to a great extent __ to some extent __to a small extent __no

Please provide additional information about yourself:
Age _____
Gender ______
Number of college credits completed ______
Major or program of study ________________________________
The number of computing devices (including smartphones and mobile devices) owned _________

Date: _____________
Name (optional) ____

References:

Caulkins, B. D., Badillo-Urquiola, K., Bockelman, P., & Leis, R. (2016, October). Cyber workforce development using a behavioral cybersecurity paradigm. In *Cyber Conflict (CyCon US), International Conference on* (pp. 1-6). IEEE.

Champion, M., Jariwala, S., Ward, P., & Cooke, N. J. (2014, September). Using Cognitive Task Analysis to Investigate the Contribution of Informal Education to Developing Cyber Security Expertise. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 58, No. 1, pp. 310-314). Sage CA: Los Angeles, CA: SAGE Publications.

Goodwin, B. (2005). Investment in security training on the wrong track, say senior staff. *Computer Weekly*, *29*.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2005). 2005 CSI/FBI computer crime and security survey. *Computer Security Journal*, *21*(3), 1.

Jansson, K., & von Solms, R. (2013). Phishing for phishing awareness. *Behaviour & Information Technology*, *32*(6), 584-593. doi:10.1080/0144929X.2011.632650.

Kim, P., & Homan, J. V. (2012). Measuring the effectiveness of information security training: a comparative analysis of computer-based training and instructor-based training. *Issues in Information Systems*, *13*(1), 215-224.

Lomo-David, E., & Shannon, L. J. (2009). Information systems security and safety measures: the dichotomy between students' familiarity and practice. *Journal of Management Information and Decision Sciences*, *12*(1/2), 29. Retrieved from

McGettrick, A., Cassel, L. N., Dark, M., Hawthorne, E. K., & Impagliazzo, J. (2014, March). Toward curricular guidelines for cybersecurity. In *Proceedings of the 45th ACM technical symposium on Computer science education* (pp. 81-82). ACM.

Muhirwe, J., & White, N. (2016). Cybersecurity awareness and practice of next generation corporate technology users. *Issues in Information Systems*, *17*(2).

Paulsen, C., McDuffie, E. L., Newhouse, W. D., & Toth, P. R. (2012). NICE: Creating a Cybersecurity Workforce and Aware Public. *IEEE Security & Privacy*, *10*(3).

Robinson, L., Brown, A., & Green, T. D. (2010). *Security vs. access: Balancing safety and productivity in the digital school*. International Society for Technology in Education.

Scheponik, T., Sherman, A. T., DeLatte, D., Phatak, D., Oliva, L., Thompson, J., & Herman, G. L. (2016, October). How students reason about Cybersecurity concepts. In *Frontiers in Education Conference (FIE), 2016 IEEE* (pp. 1-5). IEEE.

Singer, P. W., & Friedman, A. (2014). Cybersecurity: what everyone needs to know. Oxford University Press.

Stark, A. (2017). *An examination of information security training and education for IT professionals in a community college: A case study* (Order No. 10270030). Available from ProQuest Dissertations & Theses Global. (1933023362). Retrieved from https://draweb.njcu.edu:2055/docview/1933023362?accountid=12793

Teer, F. P., Kruck, S. E., & Kruck, G. P. (2007). Empiracal study of students' computer security practices/perceptions. *Journal of Computer Information Systems*, *47*(3), 105-110.

Tyworth, M., Giacobe, N. A., Mancuso, V., & Dancy, C. (2012, March). The distributed nature of cyber situation awareness. In *Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), 2012 IEEE International Multi-Disciplinary Conference on* (pp. 174-178). IEEE.