Emily Vandalovsky

Project 2 – Qualitative Study

EDTC 806 – Research Methods

Spring 2018

Dr. Carnahan

Chapter 1 – Introduction

Overview

As the number the Internet users grows every year, the incremental amount data resides at and travels through cyberspace. With it, increase the volume, magnitude and the frequency of cyber attacks (Robinson, Brown & Green, 2010, pp. 56-58). Every system is vulnerable, and therefore needs to be secured and protected by powerful and sustainable mechanisms.

Over the years, some educational institutions and professional organizations committed to providing focused technical training, which helped with educating and supplying skilled working professionals in the field (Caulkins, Badillo-Urquiola, Bockelman & Leis, 2016). However, more attentions needs to be paid to non-technical side of system protection mechanism, mostly attributed to systems users and their online behaviors.

Statement of the Problem

Securing and protecting systems cannot be asole responsibility of the industry professionals devoted to administrating and maintaining computing devices and networks. The cybersecurity awareness is a common responsibility, shared by all users on the system, on both civil and personal levels (McGettrick, Cassel, Dark, Hawthorne & Impagliazzo, 2014). For users to become more aware of cyber threats and act accordingly, their mentality needs to change (Robinson, Brown & Green, 2010, pp. 66).

Although the cybersecurity awareness has been identified as a trend for a few decades, it remains an active topic in education and in the industry, as the amount of cyber attacks continues to grow every year (Robinson, Brown & Green, 2010, pp. 56-58). All socio-economic sectors, including industry, government, and academia, share the common goal of creating and mainlining the environments, robust enough to withstand cyber attacks.

In doing so, an organization is recommended to make basic security part of their culture and “make people your first line of defense” (Verizon, 2018). In doing so, company’s employees should be able to recognize and report the warning signs of suspicious system activity.

Purpose

While there is no absolute scale for measuring the level of cybersecurity awareness in an organization, there is always room for continued vigilance and improvement. The increased level of awareness is connected to lead to the change in mentality and exhibited online behaviors (Stark, 2017). Improved security behaviors and practices contribute to strengthening the defense against cyber attacks.

The central phenomenon of this qualitative study is cybersecurity awareness as a part of an organizational culture (Creswell, 2014, p.130). The purpose of this study is to explore the current state of the cybersecurity awareness as a part of the institutional culture in one community college in the northeastern United States. The study is intended to describe participants’ perception of awareness and their role in the overall cyber well-being of the institution. It will also explore how participants feel about potential changes in the institutional cyber culture, should they occur.

Research Questions

Within the framework of the study, the following central question will be researched:

Central Question: What is cybersecurity awareness to the eight members of the college community?

Also, the following subquestions will be researched:

Subquestion 1: What does institutional culture mean?

Subquestion 2: What are the perceptions associated with the change of the institutional culture?

Subquestions 3: What are the perspectives of the community members of their role in the cyber well-being of the institution?

Limitations, Delimitations, Assumptions

Some parts of the study may include elements beyond the researcher's control, or limitations (Shamburg & Rabinovich, 2016). They include incomplete or dishonest answers or participants' unwillingness to share their insight. They may also include an inability to obtain needed documents from IT department or unexpected delays in IRB paperwork.

There are several delimitations to this study or the boundaries within which the study is performed (Shamburg & Rabinovich, 2016). The foremost delimitations have to do with the choice of topic and the setting, both of which are fairly familiar to the researcher, which may lead to some personal bias. Another delimitation is the size and the make-up of the sample. While every effort will be made to make the sample as diversified as possible, some overlaps may be possible. Additional delimitations are setup on the number of credits students earned, the number of semesters faculty and staff have been employed, the time duration of the log files IT provides.

To proceed with the flow of the study, the following assumptions will be have made. For the purposes of the study, the cybersecurity awareness topics may contain discussions on identity theft, social engineering, phishing, computer viruses (Nyabando, 2008). There are other topics included in the umbrella of cybersecurity which will remain beyond the scope of the study.

Another assumption is being made about all interviewed individuals being comfortable providing their opinions on the topic.

Chapter 2 - Literature Review

There are multiple definitions of the term cybersecurity exist, as it could be interpreted in a variety of ways. The area of cybersecurity is extensive and inclusive of protection of cyberspace, which consists not only the backbone infrastructure of the computers, their networks, hardware, software and the channels of data communication but also of people directly involved in maintaining and using all of those. According to Singer & Friedman (2014), "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).

In the recently published by Verizon Enterprise 2017 Data Breach Investigations Report (DBIR), Verizon confirms over 40,000 cybersecurity incidents, 1,935 of which resulted in data breaches (Verizon, 2018).   To clarify, a cybersecurity incident is an occurrence of unauthorized access, with potential exposure to otherwise protected assets, while a breach is a confirmed disclosure, as opposed to potential, of data to an unauthorized user (Verizon, 2018).

While no system is 100% protected from the cyber attacks arriving from different angles, the human component of cybersecurity continues to be one of the biggest contributing factors to systems exploits and information leaks (Champion, Jariwala, Ward & Cooke, 2014).   For example, as outlined in 2017 Data Breach Investigations Report, 68% of all data breaches in healthcare alone have internal causes (Verizon, 2018), which means that they have been initiated, intentionally or intentionally, by the employees or authorized users of the system. According to Goodwin (2005), internal threats could be remediated if a community of users improved their "poor user security behavior" (Goodwin, 2005).

From the social norms perspective, the cybersecurity awareness is similar to the public health awareness (Mulligan & Schneider, 2011), when every resident of the modern digital age needs to be knowledgeable about and follow appropriate social norms. Akin to the norms of personal hygiene, the rules of common digital hygiene provide a valuable foundation in the fight against cyber attack and attackers (Paulsen, McDuffie, Newhouse & Toth, 2012), as their number continues to grow.

Verizon reports that in 2017, in the area of education, there were 455 reported incidents, out of which 73 were confirmed with data disclosure (Verizon, 2018). It conjunction with the additional piece of statistics stating that "95% of phishing attacks that lead to a breach were followed by some sort of software installation" (Verizon, 2018), the cybersecurity awareness and behavior in an educational institution becomes the topic of interest and further investigation.

Some studies have been completed on how cybersecurity awareness training is related to rationalized exhibited secure behaviors (Kim & Homan, 2012; Scheponik et al., 2016; Tyworth et al., 2012; Jansson von Solms, 2013; Stark, 2017).

Chapter 3: Methodology

Introduction

Since the human factor remains one the critical points in preventing cybersecurity attacks (Champion, Jariwala, Ward & Cooke, 2014), this paper contributes to the ongoing effort to explore the levels of cybersecurity awareness in the area of higher education. The literature supports the inadequate level of attention to the human element in cyberspace as opposed to the technical component (Caulkins et al., 2016).

The study was designed to explore a phenomenon of cybersecurity awareness among the population of the community college, such as student body, faculty, staff, and administration. .

Research Design

The basic interpretive qualitative research design is appropriate for this study due to the following reasons. The concept of cybersecurity awareness may be interpreted in a variety of ways, and the exploratory nature of the study will allow the researcher to have a more detailed conversations of the topic and discover various interpretations. Of the particular importance will be participants' perceptions of their role in the cyber well-being of the institution and on changes in the cyber culture of the college.

The main data collecting tool for this study was a sequence of scheduled interviews. The interviews were conducted with eight representatives from the college community, as outlines in the section below. To assist with the data analysis, the interviews were recorded, of course with the permission of the interviewee. External auditor and members checks were later used to establish validity and reliability of the study. According to Cresswell (2014), the reliability of the study is evaluated when the research technique yields the same results. Validity measures how accurate and realistic the findings are (Cresswell, 2014).

Population and Sample

The intent of this study is to explore a phenomenon of cybersecurity awareness among the population of the community college. To perform an in-depth exploration from a multi-perspective viewpoint, the maximal variation design of the purposeful sampling will be used in the study. It will allow representation from various constituencies of the college. The participants' role in the college community will be a defining characteristic within the sample. The following groups will be represented within the sampling: student body, faculty, non-IT staff, and administration. Each group will be represented by the two participants, totaling in the sample size of eight people. The best attempt will be made to identify representatives from the various subgroups within a group.

The intended sampling of each group will be created as follows. Considering that students need to earn 62-64 credits for an associate level degree, one student representative will have between 16-31credits, representing the freshman class, but eliminating first-semester group, who may not be yet as familiar with some college practices. The second student representative will have over 32 credits earned, representing the sophomore-level class. Additionally, one of the students will be enrolled in a Liberal Arts degree program, while the other one will be majoring in one of STEM programs. Non-essential to the findings of this study, but students will be of different ages, genders and ethnic backgrounds. No attention will be paid to the full-time vs. part-time status of the student participant, which may create a limitation to the study, as further discusses.

Similar criteria will be considered in selecting representatives for the faculty group. One faculty member will be from Liberal Arts area, while the other one will be from STEM area. One faculty will be full-time and tenured, which means that they have worked at the college for at least five years. The other faculty member will be part-time (or adjunct) and will have to be continuously teaching for at least two full semesters. Akin to the introductory college experience of freshmen, novice adjunct faculty members may not be as familiar with some college practices. Just like with student body, strong consideration will be given to selecting faculty of different ages, genders, and ethnical backgrounds.

In selecting two staff members a special consideration will be made to focus on non-IT representatives since the topic of this study is directly connected to the everyday job responsibilities of some IT employees, their opinions may introduce additional bias. Furthermore, IT department plays a special role in the study, related to obtaining needed documents, so IT's participation is instrumental and valuable.

The two non-IT staff members will be selected from two large areas: one is from the student services area, and the other one is from the institutional support area. Both selected participants will be employed at the college for at least two years and will come from the various levels of the organizational chart. One representative will be a lower-level staff member with limited responsibilities, while the other one will hold a supervisory position. As previously stated, every attempt will be made to select representatives of different ages, genders and ethnic backgrounds, but since these factors are not of particular interest of the study, they will be noted, but not analyzed.

The last two participants of the study will represent the administrative circle of the institution. One representative will come from the academic area, while the other one will be overseeing non-academic infrastructures. Due to the higher level positions, occupied by these individuals, no special consideration will be given to the years on the job. As with other categories, every attempt will be made to select representatives of difference ages, genders, and ethnic backgrounds.

Researcher’s Position

Since this study will not incorporate any observations, the researcher’s position will be mostly non-participatory. The researcher will conduct a series of individual interviews with the study participants and request some documents from the institutional IT department.

In case of the researcher being employed at the same educational institution that she is studying, the researcher-participant relationship may play a role. The friendly type of relationship may positively impact the interviews and willingness of participants to share their insight. The lack of pre-existing collegial relationship between a participant and the researcher may negatively impact the study where participants may lack enthusiasm and willingness to provide detailed answers.

The researcher will confirm the complete confidentiality of the acquired information, will stress the non-judgmental nature of the study and will encourage honest and complete participation. The researcher will remind participants of the importance of their contribution to this particular study and the overall exploration of the cybersecurity awareness levels among the college population.

The researcher’s interests in conducting this study lay within the framework of the researchers’ interested in cybersecurity awareness in general. This research may become a useful piece of information about the current state of cybersecurity awareness at the particular institution. Depending on its finding, it may propose additional in the topic to the constituencies of the college.

Due to the exploratory nature of the research and the limited number of the sample size, the researcher is relying on the assumption that experiences shared by the interviewed participants will be similar to the other members of the same group, such as students, faculty, staff, and administration. The researcher is also counting on the fact that provided answers will be truthful and thorough.

Since the researcher is somewhat familiar with the topic of cybersecurity awareness, she will have pay special attention to the personal bias and opinions not affecting the study, and especially so during the interview sessions.

Procedures

Before collecting data, I would seek approval of the Institutional Review Board, for which I will develop the description of the project, consent form, and the project outline (Creswell, 2014, p.209). Upon approval from IRB, I will start reaching out to participants for scheduling one-on-one interviews.

This study will not include observations and will rely on the following types of qualitative data: interviews, documents and audio materials (Creswell, 2014, p.211). The interviews will start with one closed-ended question, which will be followed by the open-ended questions (Creswell, 2014, p.219). The sample interview questions are listed below.

Question 1 (closed-ended): please specify the extent of your agreement or disagreement with this statement: “Cybersecurity Awareness and Practice should be limited to professionals who administer and support computing devices.”

_______ Do you strongly agree?
_______ Do you agree?
_______ Are you undecided?
_______ Do you disagree?
_______ Do you strongly disagree?

Question 2 (open-ended): please indicate the reasons for selecting your response.

Question 3 (open-ended): please elaborate on what does cybersecurity mean to you? Provide examples, if any.

Question 4 (open-ended): how do you perceive your role in the overall cyber well-being of the college?

Question 5 (open-ended): what was your experience with identity theft, social engineering, phishing emails, dealing with computer viruses, creating and storing passwords?

Question 6 (open-ended): what does the college’s cyber culture mean to you and how would you feel about changing it if necessary?

In addition to conducting one-on-one interviews and audiotaping them (with the prior consent the participant), I will collect a number of technical documents. I will work with IT department to obtain automatically produced log files specifying any suspicious activity on the system. I setup the delimitation of six month period for the log files to review. I would also request the system reports on any phishing attack occurrences within last six month. If possible, I would obtain reports users recognizing and deleting a phishing email vs. the ones who downloaded it or forwarded further.

Having the automatically produced system logs will allow to better understand the realistic state of the cybersecurity at the college, and compare the interpretation of the results with the answers supplied by interviewees.

Bibliography:

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.

Creswell, J. (2014) *Educational Research: Planning, Conducting, and Evaluating Quantitative and Qualitative Research*. Pearson.

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

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

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.

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.

Mulligan, D. K., & Schneider, F. B. (2011). Doctrine for cybersecurity. *Daedalus*, *140*(4), 70-92.

Nyabando, C. J. (2008). *An analysis of perceived faculty and staff computing behaviors that protect or expose them or others to information security attacks* (Doctoral dissertation, East Tennessee State University).

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.

Shamburg, C. & Rabinovich L. (2016) *Guidelines for the qualitative methods dissertation* (Draft). Jersey City, NJ: Department of Educational Technology, New Jersey City University.

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

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.

Verizon (2018). 2017 Data breach investigations report. *Report, Verizon Enterprise*. Retrieved from http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

Additional Resources from Project #1:

Creswell, J. (2014) *Educational Research: Planning, Conducting, and Evaluating Quantitative and Qualitative Research*. Pearson.

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

Mulligan, D. K., & Schneider, F. B. (2011). Doctrine for cybersecurity. *Daedalus*, *140*(4), 70-92.

Nyabando, C. J. (2008). *An analysis of perceived faculty and staff computing behaviors that protect or expose them or others to information security attacks* (Doctoral dissertation, East Tennessee State University).

Shamburg, C. & Rabinovich L. (2016) *Guidelines for the qualitative methods dissertation* (Draft). Jersey City, NJ: Department of Educational Technology, New Jersey City University.

Verizon (2018). 2017 Data breach investigations report. *Report, Verizon Enterprise*. Retrieved from http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/