Emily Vandalovsky

Project 3 – Mixed Methods Study

Perception of Cybersecurity Awareness: An Examination Community College Students' Understanding of the Concept of Cybersecurity Awareness and Online Behaviors

EDTC 806 – Research Methods

Dr. Carnahan

Spring 2018

Introduction

To withstand the ever-growing magnitude, volume and frequency of cyber attacks (Robinson, Brown & Green, 2010, pp. 56-58), the field of cybersecurity continues to develop and expand. With its encompassing nature and complexity of applications, it crosses the boundaries of the technical areas, including but not limited to technological fluency, data and network security, information assurance and encryption, onto the non-technical areas, such as privacy, policy, behavioral and social psychology, communication and many others.

Cybersecurity is not just a multidimensional phenomenon that mandates a multilayered methodology, but also a complex, continually developing zone that requires an up-to-date complex approach for studying it. Since the mixed methods research design is the most inclusive and emergent of all designs (Creswell & Clark, 2018), it provides an adequate toolset for conducting a study in the area of cybersecurity.

Statement

Since the protection and security of information systems and data is everybody's responsibility, the commonly used mechanisms of the cybersecurity awareness should be regularly employed by all computer users on the personal and civil levels (McGettrick, Cassel, Dark, Hawthorne & Impagliazzo, 2014). While the computerized systems keep on developing and providing new technological levels of protection, the human element of cybersecurity remains one of the leading causes of information leaks and cyber breaches (Champion, Jariwala, Ward & Cooke, 2014). Some of these leaks or breaches could be prevented by the community of users were more knowledgeable about cybersecurity awareness and improved their "poor user security behavior" (Goodwin, 2005).

In the recently published 2017 Data Breach Investigations Report, Verizon confirms 455 incidents in the field of education, 73 of which resulted in the unauthorized data disclosure (Verizon, 2018). By combining it with another piece of data from the same report 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 safe online behavior among student population emerges as a topic of interest for conducting further research. Moreover, the existing literature exhibits a deficiency in this area, and even to the greater extent, in the community college educational sector.

Purpose

The purpose of this study is to explore the current state of cybersecurity awareness and perceived online behaviors among the student population in one community college in the northeastern United States. An exploratory sequential design will be used first to explore qualitatively to develop a context-specific and sensitive questionnaire on cybersecurity awareness and perception that will be quantitatively tested. The first phase of the study will be a qualitative exploration of the cybersecurity awareness and perceived online behaviors in which interview-based data will be collected from a group of students. From this initial exploration, the qualitative findings will be used to develop a questionnaire that can be administered to a large sample of the student community. In the tentatively planned quantitative phase, the survey will be collected from freshmen at the same college to measure the prevalence of the developed instrument (adapted from Creswell & Plano Clark, 2018).

Research Questions

The following research questions will be addressed in this study:

Question 1: What is cybersecurity awareness to the students of the community college?

Question 2: What is the perception of the safety of the online behaviors exhibited by the community college students?

Question 3: Are the themes of cybersecurity awareness and perceived online behaviors generalizable to the community college student population?

Limitations

The study contains several limitations, related to various factors. One of the risk factors is associated with the nature of the design when the success of the first phase drives the success of the second phase of the study. Another limitation has to do with the researcher's preconceived bias on the topic, which may influence the development of the instrument.

The limitation in selecting sampling from the students in a particular major and enrolled in a particular course may limit the scalability of the study to other institutions, where such major or course may not be available.

Literature Review

Mixed methods research design provides an inclusive framework for studying complex and multifaceted phenomena. By incorporating the strength and advantages of both the qualitative and quantitative methods, a mixed methods approach allows investigating the topic further not only to study why and how does the phenomenon occur, but also attempt to create generalizable conclusions based on empirical data (Smith, Cannata & Haynes, 2016).

Below are several examples of the mixed studies research studies conducted in the area of cybersecurity and related to the cybersecurity awareness. Each of them provides learning opportunities and areas for improvement in conducting a mixed methods research under the cybersecurity umbrella.

In her doctoral dissertation, Chiwaraidzo Nyabando studied perceived computing behaviors associated with protection against or exposure to the cybersecurity attacks (Nyabando, 2008). The study was conducted using the mixed methods approach. The literature review section of this study was compiled in a very rational, orderly way, starting with the chronological perspective on the issues from the 1960s to the present, followed by the three sections that provided the core theoretical framework, and concluded with the section on the best practices (Nyabando, 2008). Such regimental structure to the literature review is advantageous to both the researcher and the readers due to the complexity and technical applicability of the topic.

Nyabando refers to Snyder (2006) while defining the design of her study as triangulation, when "[q]ualitative and quantitative data are collected and analyzed simultaneously" (2008). According to Creswell & Plano Clark (2018), this approach is considered convergent. Such discrepancy in topologies provides further evidence that the mixed methods research design continues to develop and undergo revisions. The revisions are subject to the field of study and

the authors' interpretation (Creswell & Plano Clark, 2018). A special attention must be paid to the discrepancies in the vocabulary of the published literature, with an extreme focus on the publication year and the area of research.

Nyabando presented qualitative and quantitative data independently and implemented the constant comparison method in the data analysis (2006). The researcher stresses the levels of validity due to triangulation and constant comparison. It appears that the study was thoroughly conducted within the frameworks of the convergent design and that the conclusions were drawn based on the well-aligned approaches and research questions.

In their study on the information security effectiveness, Knapp, Marshall, Rainer Jr. & Ford used a sequential qualitative quantitative methodological approach to propose and test a theoretical model (2007). The study employed six step methodological process, combining the following techniques: qualitative data collection, qualitative analysis, scale development, instrument refinement, quantitative data collection, and quantitative data analysis (Knapp et al., 2007).

The researchers followed a grounded theory approach in using quantitative strategy to develop a theoretical model. In this model, the theory is discovered through the findings rather than existing literature (Creswell, 2014). Creswell and Plano Clark attribute a grounded theory framework to the exploratory sequential mixed methods design. In this approach, the emerging theory, grounded with the input from the participants, may contribute to the further examined variable or a developed instrument (2018).

Once the theoretical model emerged, Knapp et al., developed a survey and tested it using structural equation modeling (SEM) software. An alternative structural model was also created.

To raise credibility to the study, the researchers discussed their findings and linked them to previously conducted research and existing theories (Knapp et al., 2007).

One of the study limitations includes the use of self-reporting mechanisms for data gathering and measuring. With the focus of the study of the information security, the respondents may be hesitant to honestly report on security ineffectiveness to avoid negative perception or publicity (Knapp et al., 2007).

Another limitation is related to the generalizability of the findings. During the first (qualitative) step of the study, the data was collected from 220 Certified Information Security Professionals (CISSPs), all of whom were highly qualified individuals with at least three years of professional experience in the field (Knapp et al., 2007). While their feedback could be considered expert opinion, the grounded theory derived from it must recognize the homogenous nature of its sample population.

Special considerations must be given while generalizing the theory to other industries and social environments (Knapp et al., 2007). Although information security is globally recognized phenomenon, before generalizing its theoretical model, the sample, representative of a different culture or organization, should be selected and employed.

In their study on the perception of the information security, Huang, Rau, and Salvendy employed multiple research methods to investigate people's perception of it and further explore its relationship to other factors (2010). Although the study has not been formally identified as mixed methods, it employed the elements of both, the quantitative and qualitative approaches.

Based on the literature related to the topic, Huang, Rau, and Salvendy derived the 20-question survey listing the items that may influence users' perceptions of information security.

Independently, the open-ended, in-depth questionnaire was presented to twenty university students, who, according to the team of researchers, "had abundant computer and Internet experience" (Huang, Rau & Salvendy, 2010). The answers extracted from the questionnaire validated the contents of the survey and allowed for two additional categories, which were further investigated within the revised framework of the research.

The updated version of the survey was made available to all visitors of IT Usability Laboratory website at Tsinghua University, China. Out of 646 responses, 44 were found incomplete or inconsistent, bringing the total count of valid responses to 602 (Huang, Rau & Salvendy, 2010). It would be helpful to know what kind of inconsistency the researchers found invalid. The answers could be found inconsistent for valid reasons or, possibly, represent an oddity in the data set or cause additional inconvenience for the data analysis. The limitations section of the study offers no further explanations.

Other limitations of the study are related to the specification of the timing and the selection of the sampling for the quantitative component, both of which contribute to the generalizability of the findings. No information was provided about how long the survey was made available on the website and how the website visitors learned about it. Also, were the potential visitors encouraged or required in some way to complete it, and, more importantly, whether or not the visitors to IT Usability Laboratory website can represent a fair sampling of all students of Tsinghua University.

The study resulted in the six-factor structure on people's perception of the information security threats. The model of the structure derived from the survey and exploratory factor analysis. The relationship between the factors and their effect on the overall perception of threats were established and evaluated by multiple regression analysis. The perception of the

information security was found significantly related to the user's computer experience and the type of loss that the threat could bring. The type of loss was presented by Huang, Rau & Salvendy as a multiple choice from the following categories: "financial loss, exposure of personal information, inconvenience of computer use, waste of time, loss of reputation and loss of data" (2010).

While the study employs both the quantitative and the qualitative methods for data gathering and analysis, it was not specified what type of the mixed methods framework it follows. Although the study provides ample reference points to the published literature, it does not appear to link to any existing theories. In my understanding, the design of this study employs the exploratory sequential mixed methods approach.

Upon evaluating existing studies related to the topic of cybersecurity awareness and perceived behaviors among community college students, the gap in the published literature was identified. It promoted the need for further exploration of the topic with the possibility of developing the measurement instrument for such. The exploratory sequential design deemed as the appropriate methodology for accomplishing it.

Methodology

Since the exploratory sequential design starts with and emphasizes the substantial qualitative component, it allows the researcher to explore a multitude of perspectives and the depth of the focus area. The qualitative methods strongly relate to the constructivists worldviews (Creswell & Plano Clark, 2018). In the immediately following phase of the research characterized by the elements of the quantitative design, such as measuring variables and employing statistical mechanisms, the postpositivist philosophical worldviews are replaced by the constructivist theory. In the final phase of the design, such as data interpretation, either one of the theories (postpositivist or constructivist) or "a dialectical perspective involving both stances" could be presented (Creswell & Plano Clark, 2018, p. 86). The exploratory sequential design is rich not only with employing multiple worldviews but also with an ability to move from one worldview to another.

The topic of cybersecurity with its encompassing and multifaceted nature fits well into the framework of the mixed method design approach. The exploratory sequential design allows for the magnitude of worldviews, capable of representing the wealth and complexity of the cybersecurity awareness perceptions.

Research Design

The exploratory sequential design can be viewed as a three-phase study resulting in a newly developed and tested instrument (Enosh, Tzafrir & Stolovy, 2015). The first phase contains a qualitative component, the results of which are recorded and further used in the second phase. During the second phase, the researcher analyses qualitative data from the first phase and extracts quantitative elements out of it. This process contributes to the development of

the instrument used in the following, the third phase of the study. The third phase contains the quantitative data collection and analysis, which focuses on testing or generalizing the initial qualitative findings from the first phase (Creswell & Plano Clark, 2018).

In this type of design, the qualitative component carries the heavier weight, as it performs the initial exploration into the topic, which later serves as a foundation for developing and testing the instrument in the follow-up phases. Since the framework of this design assumes the dependency of the quantitative component on the effective execution of the initial qualitative component, the success of the entire study is dependent upon the effectiveness of the qualitative piece.

The exploratory sequential design is the lengthiest of all mixed methods core design approaches, as it requires adequate time to conduct the three distinct phases of the study in the strictly sequential order (Creswell & Plano Clark, 2018). The timing of this study will span over the two consecutive semesters, with the break between them dedicated to the development of the new instrument.

Population and Sample

Since this study is constructed in a multi-phase approach, the data collection for each phase uses its method for selecting population sample. With the first phase of the study being of the qualitative nature, the purposeful sampling will be used. For the quantitative phase, the random sampling of the greater order will be implemented.

Since the intent of the first phase of the study is to explore the cybersecurity awareness and perceived behaviors among the community college students, the purposeful sampling of the student body will be implemented using the following rationale and assumptions.

The cybersecurity awareness is the elementary level of the cybersecurity field, which further incorporates network security and other implications of the computer security areas. Community college students pursuing a degree in Network Administration are exposed to the topics on cybersecurity within the coursework of the program. Among the general student population, network administration students may be considered as "student experts" in the field of cybersecurity due to the nature of their course of study.

The purposeful sampling for the qualitative phase of the research will contain all students majoring in network administration program during their last semester before graduation. The aim for the sample size is to contain twenty to thirty participants, all of whom are declared network administration majors, enrolled in their last semester before graduation.

Since the mixed methods exploratory sequential design resembles the qualitative grounded theory approach, it is important to consider the point of saturation. Once the data is collected and analyzed and the researcher can no longer extract new themes or new characteristics from the responses, the point of saturation in data gathering is reached, and the sufficient sample is obtained (Charmaz, 2006).

For the quantitative phase of the study, the random sampling will be used. A copy of the newly constructed survey will be emailed to all students at the college currently enrolled in the Introduction to College experience class. By doing so, the following objectives on the student population selection will be met: 1) the students receiving the survey are freshmen, since the Introduction to the College experience course must be completed within the first academic year; 2) the students from all majors and programs of study are enrolled in the Introduction to the College experience course, thus randomly representing the entire student body. Using this selection criteria, the anticipated population size is to include over 200 students.

In the exploratory sequential design, it is important not to engage the same participants into the qualitative and quantitative phases of the study since the exposure to the initial questionnaire may influence the responses to the developed instrument and jeopardize the validity of the instrument. By selecting the graduating students for the qualitative part and first-year students for the quantitative part, the two samples should have no overlaps, and therefore enhance the generalization of the results. Moreover, since the data collection stage will span over the two consecutive semesters, starting with the graduating students in semester one, and follow up with the first-year students in semester two, the two population samples will not overlap.

Procedures

Before the data collecting state, the approval from the Institutional Review Board (IRB) will have to be warranted. The application for approval will contain the description of the project, the participant's consent form and the project outline (Creswell, 2014). Once the IRB approval is received, the participants may be contacted, and the data collection may begin.

The first part of the study will employ a qualitative approach and will produce data of the following types: interviews and audio materials (Creswell, 2014). The interviews will begin with one close-ended question, followed by the four open-ended questions and conclude with one restricted open-ended question. The listing of the interview questions is presented in Appendix A. The answers to these questions will be recorded using a recording device (with prior consent from participants) and later used for the data analysis phase.

The initial selection of the purposeful sampling along with the data collection stage will take one semester to complete, provided that at least twenty individual interviews need to be

scheduled. Since this part of the study carries the heavier weight, is it important to carefully administer it and follow the established schedule.

The data obtained from the interviews will be recorded. The emerging themes, specified by the respondents, will be observed and categorized, to be followed by the process of integration. According to Creswell & Plano Clark, "[i]ntergration involves using the qualitative results (e.g,. themes and significant statements) to build a new quantitative feature that is grounded in the culture and perspective of participants. This feature is then quantitatively tested" (2018).

The data collected from the interviews will be analyzed using content analysis procedure. The content analysis procedures assist with dividing the text into more practical units, such as themes, phrases, and words (Haber, 2012). By implementing explicit coding, the thematic content analysis allows drawing reliable and valid conclusions (Krippendorff, 2004), which could be further used to create a quantitative feature.

Depending on the type of the quantitate features developed in the second phase of the study, Creswell & Plano Clark recognize four variants of the exploratory sequential design, such as new variable development variant, survey-development variant, intervention-development variant and digital tool development variant (2018). This study will implement the survey-development variant which, once created, will be tested in practice among the student population.

The estimated time of eight weeks will be allotted for the second phase of the study, dedicated to the development of the quantitate element. This phase will culminate in the newly developed twenty-question survey with the following foci in mind: (1) questions on the

understanding of the cybersecurity and its awareness; (2) questions on the perceptions of the online behavior; (3) questions related to the cyber well-being of the college and the role of individual students within it; (4) questions on perceived importance of acquiring specific cybersecurity skills, knowledge and behaviors. Additional types of questions will be considered based on the processed qualitative data.

The third phase, scheduled for the following semester, will focus on administering the survey and collecting the results from it. The survey will be distributed to all students enrolled in the Introduction to College experience course, with an estimated sample size of over 200 students. The students will complete the survey in the electronic format delivered through the college's online learning system.

Research Question	Data Type	Source of data
What is cybersecurity awareness to the students of the community college?	Qualitative, text-based Quantitative	Interview, audio recording Survey
What is the perception of the safety of the online behaviors exhibited by the community college students?	Qualitative, text-based Quantitative	Interview, audio recording Survey
Are the themes of cybersecurity awareness and perceived online behaviors generalizable to the community college student population?	Quantitative	Survey

Appendix A

Interview Questions for the Qualitative Phase	
Question 1 (close-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 to Question 1.
Question 3 (open-ended):	Please elaborate on what does cybersecurity mean to you? Provide examples.
Question 4 (open-ended):	Do you perceive your online behavior as safe? Provide examples.
Question 4 (open-ended):	How do you perceive your role in the overall cyber well-being of the college? Provided the opportunity, what would you change about it?
Question 5 (restricted open-ended):	What was your understanding and/or experience with any two of the following phenomena: identity theft, social engineering, phishing emails, computer viruses, creating and storing passwords, mobile cybersecurity?

References:

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.

Charmaz, K. (2006). *Constructing grounded theory*. Thousand Oaks, CA: Sage.

Creswell, J. (2014). *Educational Research: Planning, Conducting, and Evaluating Quantitative and Qualitative Research*. (5th Ed.). Boston, MA: Pearson.

Creswell, J. & Plano Clark, V. (2018). *Designing and Conducting Mixed Methods Research (*3rd Ed.) Los Angeles, CA: SAGE Publications.

Enosh, G., Tzafrir, S. S., & Stolovy, T. (2015). The development of client violence questionnaire (CVQ). *Journal of Mixed Methods Research*, *9*(3), 273-290.\

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

Haber, P. (2012). Perceptions of leadership: An examination of college students' understandings of the concept of leadership. *Journal of Leadership Education, 11*(2), 26-51.

Huang, D. L., Rau, P. L. P., & Salvendy, G. (2010). Perception of information security. *Behaviour & Information Technology*, 29(3), 221-232.

Knapp, K. J., Marshall, T. E., Rainer Jr, R. K., & Ford, F. N. (2007). Information security effectiveness: Conceptualization and validation of a theory. International Journal of Information Security and Privacy (IJISP), 1(2), 37-60.

Krippendorff, K. (2004). *Content analysis: An introduction to its methodology* (2nd Ed.). Thousand Oaks, CA: Sage.

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.

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). Retrieved from https://dc.etsu.edu/cgi/viewcontent.cgi?article=3324&context=etd

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.

Smith, T. M., Cannata, M., & Haynes, K. T. (2016). Reconciling Data from Different Sources: Practical Realities of Using Mixed Methods to Identify Effective High School Practices. *Teachers College Record*, *118*(7), n7.

Snyder, A. L. (2006). Mixed-method designs. In J. H. McMillan & S. Schumacher (Eds.), *Research in Education: Evidence-based inquiry* (pp. 400-420). Boston: Allyn and Bacon.

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

New References:

Charmaz, K. (2006). *Constructing grounded theory*. Thousand Oaks, CA: Sage.

Creswell, J. & Plano Clark, V. (2018). *Designing and Conducting Mixed Methods Research (*3rd Ed.) Los Angeles, CA: SAGE Publications.

Enosh, G., Tzafrir, S. S., & Stolovy, T. (2015). The development of client violence questionnaire (CVQ). *Journal of Mixed Methods Research*, *9*(3), 273-290

Haber, P. (2012). Perceptions of leadership: An examination of college students' understandings of the concept of leadership. *Journal of Leadership Education, 11*(2), 26-51.

Huang, D. L., Rau, P. L. P., & Salvendy, G. (2010). Perception of information security. *Behaviour & Information Technology*, 29(3), 221-232.

Knapp, K. J., Marshall, T. E., Rainer Jr, R. K., & Ford, F. N. (2007). Information security effectiveness: Conceptualization and validation of a theory. International Journal of Information Security and Privacy (IJISP), 1(2), 37-60.

Krippendorff, K. (2004). *Content analysis: An introduction to its methodology* (2nd Ed.). Thousand Oaks, CA: Sage.

Smith, T. M., Cannata, M., & Haynes, K. T. (2016). Reconciling Data from Different Sources: Practical Realities of Using Mixed Methods to Identify Effective High School Practices. *Teachers College Record*, *118*(7), n7.

Snyder, A. L. (2006). Mixed-method designs. In J. H. McMillan & S. Schumacher (Eds.), *Research in Education: Evidence-based inquiry* (pp. 400-420). Boston: Allyn and Bacon.