2019

Cybersecurity Strategies for Universities With Bring Your Own Device Programs

Hai Vu Nguyen
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Hai Nguyen

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Gail Miles, Committee Chairperson, Information Technology Faculty
Dr. Jose Feliciano, Committee Member, Information Technology Faculty
Dr. Steven Case, University Reviewer, Information Technology Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2019

Abstract

Cybersecurity Strategies for Universities With Bring Your Own Device Programs

by

Hai Vu Nguyen

MS, Walden University, 2017

MIS, University of Phoenix, 2009

BA, University of California, Davis, 1999

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

December 2019

Abstract

The bring your own device (BYOD) phenomenon has proliferated, making its way into different business and educational sectors and enabling multiple vectors of attack and vulnerability to protected data. The purpose of this multiple-case study was to explore the strategies information technology (IT) security professionals working in a university setting use to secure an environment to support BYOD in a university system. The study population was comprised of IT security professionals from the University of California campuses currently managing a network environment for at least 2 years where BYOD has been implemented. Protection motivation theory was the study's conceptual framework. The data collection process included interviews with 10 IT security professionals and the gathering of publicly-accessible documents retrieved from the Internet (n = 59). Data collected from the interviews and member checking were triangulated with the publicly-accessible documents to identify major themes. Thematic analysis with the aid of NVivo 12 Plus was used to identify 4 themes: the ubiquity of BYOD in higher education, accessibility strategies for mobile devices, the effectiveness of BYOD strategies that minimize risk, and IT security professionals' tasks include identifying and implementing network security strategies. The study's implications for positive social change include increasing the number of users informed about cybersecurity and comfortable with defending their networks against foreign and domestic threats to information security and privacy. These changes may mitigate and reduce the spread of malware and viruses and improve overall cybersecurity in BYOD-enabled organizations.

Cybersecurity Strategies for Universities With Bring Your Own Device Programs

Hai Vu Nguyen

MS, Walden University, 2017

MIS, University of Phoenix, 2009

BA, University of California, Davis, 1999

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

December 2019

Dedication

I would like to dedicate this study to my wonderful wife for being extremely supportive and understanding during my doctoral journey, my son to show him that knowledge is boundless and learning continues beyond high school and the first four years of college, and my parents for without them, I would not exist to undertake this challenge.

Acknowledgments

This journey has been a long and humbling one taking up a lot of my evening and weekend time that was originally set aside for family. First, I would like to thank my family, friends, and co-workers for their support and encouragement throughout the program. Second, I would like to thank my doctoral committee and reviewers especially Dr. Gail Miles for her superb mentorship, support, and feedback throughout the life of my study; Dr. Lawrence Ness for his support and confidence in me through the prospectus and proposal stages; Dr. Jose Feliciano for getting me through the final study stages; Dr. Steven Case for being my first Walden instructor, providing invaluable feedback at the residencies, and serving as my university research reviewer; and Dr. Tara Kachgal for being a thorough but generous form and style reviewer who help ensure that my paper met university standards. Finally, I would like to thank the participants for their time and contribution to the growing pool of knowledge. Without the support of everyone mentioned above, I would not have been able to complete this study.

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

Background of the Problem

The information technology landscape is constantly changing with new creations, innovations, and strategies designed to improve the quality of life and streamline business processes to be more effective and efficient. New devices, applications, services, and policies that have brought with them associated advantages, disadvantages, and threats. The proliferation of bring your own device (BYOD) practice in the workplace is one of these changes and has become a popular phenomenon in corporations, hospitals, and universities (Magruder, Lewis, Burks, & Smolinski, 2015).

BYOD adoption has advantages in terms of increasing productivity, efficiency, and profit and lowering costs by placing the responsibility of purchasing, maintaining, and caring for devices on the user (Pinchot & Paullet, 2015; Toperesu & Van Bell, 2017). However, it also has disadvantages. For instance, devices are easily lost or stolen. In addition, malware and antivirus protection may be lacking, placing the contents and data at risk of compromise and presenting a potential liability issue because the organization may not have legal authority to access or obtain business information or manage the security on the personal devices (Pinchot & Paullet, 2015; Toperesu & Van Bell, 2017). Cascardo (2016) explained that the average consolidated cost of data breached by cyberattacks against health care organizations in the United States in 2015, for instance, was $3.8 million.

Studies involving BYOD in education have been conducted at the elementary school through university levels, encompassing instruction to security management, and from different user and support perspectives. Researchers have examined BYOD in education from the user's perspective regarding instruction in the classroom, factors and reasons for adoption, and how BYOD may increase the security threat level (Tinmaz & Lee, 2019). However, according to my

review of the literature, they have not yet explored the strategies or methods used to manage BYOD while considering academic freedom in higher education. In conducting this research, I sought to provide greater understanding of the strategies used in managing BYOD in a statewide university system.

Problem Statement

Although the BYOD phenomenon has grown in popularity, the boundaries between personal and business use are often obscured; this presents substantial security risks and challenges for information technology (IT) security professionals (Pinchot & Paullet, 2015). In 2015, 47% of the major breaches were due to malicious attacks costing the United States $6.53 million per organization (Sebescen & Vitak, 2017). The number of mobile devices was about 8.4 billion worldwide in 2017 and is expected to reach 20.4 billion by 2020 (Meinert et al., 2018). The general IT problem is that the adoption of BYOD increases the risk of security and privacy threats in an educational environment. The specific IT problem is that some IT security professionals working in a university setting lack the strategies to secure an environment to support BYOD in a university system.

Purpose Statement

The purpose of this qualitative descriptive multiple-case study was to explore the strategies IT security professionals working in a university setting use to secure an environment to support BYOD. The research population consisted of IT security professionals from University of California (UC) campuses currently managing a network environment for at least two years where BYOD has been implemented. The results of this study may contribute to positive social change by identifying strategies for securing a network to protect the security and privacy of personal and sensitive data on the personal devices of students, faculty, and staff and on-campus servers while connected to the institution's network. The findings of this research may be

generalized to IT security practitioners in other business sectors and industries seeking to implement security on networks with BYOD devices.

Nature of the Study

I chose a qualitative descriptive multiple-case study design methodology for the study. My intent was to develop a deeper understanding of how a network allowing BYOD is secured from the perspective of an IT security professional. Using the qualitative method, researchers can observe behavior in a natural and uninhibited environment and collect more in-depth and detailed data from nonquantifiable or nonstatistical sources through a combination of notes, audio or video recordings, and interactions with participants (Jervis & Drake, 2014). In this study, I conducted interviews of multiple cases, which allowed me to interact with the participants and draw out information to better understand how the study phenomenon might influence their behavior. I also gathered publicly-accessible documents to better understand the policies that may or may not be enforced and recorded environmental factors and observations of the participants. Therefore, the qualitative method was the best approach. Use of a quantitative method, in contrast, would have required that the study be designed before collecting data. A quantitative researcher uses questionnaires and equipment as tools to collect numerical data (McCusker & Gunaydin, 2015) and then uses variables, numbers, and statistics to measure and analyze an individual's experience or causal relationships and test theories (Yilmaz, 2013). I did not collect data to assess relationships or correlations; thus, the quantitative method was not appropriate for this study. In a mixed-methods design, elements of qualitative and quantitative approaches are combined (Schoonenboom & Johnson, 2017). Because the aim of the study was to attain deeper meaning and understanding of a phenomenon from the perspective of participants, quantitative and mixed-methods approaches were not appropriate.

I used a descriptive multiple-case study approach. The narrative approach allows a researcher to explore and gain insight into a participant's experience or a story told in his or her own words (Adams, 2017). In this study, my interest was not in the life story of the participant; instead, I sought to explore the strategies employed by the participants to manage a secure network supporting BYOD; for this reason, the narrative design was not a good option. A phenomenological approach allows a researcher to examine the lived experience of participants who have experienced the same phenomenon (Byrne, 2001). The purpose of this study was not to understand how BYOD affects the participants; therefore, a phenomenological design was also not appropriate.

Ethnography is a highly inductive but flexible approach that requires that the researcher be immersed in a community and closely interact with the people in it for an extended duration of time to build a trusting relationship where rich and accurate data can be collected (Crampton, 2016). Ethnography is holistic and free-flowing, having no set process to follow, but is highly theoretical and can be used to build new theory and enhance exiting theory (Morse, 2016). This approach would be appropriate for examining the collaboration or sharing of information and knowledge between the IT security practitioners but not the actual practices in dealing with a particular phenomenon or issue. My goal was to explore the strategies employed by participants in their specific environments; therefore, ethnography was not a viable approach for this study.

Case studies are preferred when exploring *how* or *why* questions, when the researcher has minimal control over the situation, and when the phenomenon is contemporary and ongoing (Villarreal Larrinaga, 2017). A qualitative descriptive approach is grounded in the principles of naturalistic inquiry guided by an interpretive theory or conceptual framework and allows a researcher to collect data using observations, document review, or semistructured interview or focus group questions using any purposive sampling technique (Colorafi & Evans, 2016). I

collected data for this study from semistructured interviews and publicly-accessible policy and procedural documents to obtain a deeper understanding of strategies employed by IT practitioners to manage a secure network environment supporting BYOD; hence, I selected a qualitative descriptive multiple-case study approach for this study.

Research Question

The overarching research question was, What strategies do IT security professionals working in a university setting use to secure an environment to support BYOD in a university system?

Interview Questions

Using the protection motivation theory (PMT; Rogers, 1975) as the guiding framework, I developed the following open-ended questions to elicit responses that would inform the research question:

1. What are some of the factors that influenced the adoption of BYOD in your organization?
2. What types of BYOD are allowed on your network?
3. What strategies have you used to secure an environment to support BYOD?
4. How would you determine which strategies are implemented?
5. What type of information is accessible via personal devices?
6. What is involved when managing a network where BYOD is present?
7. How would you describe your role and involvement in the acquisition and implementation of the security strategies?
8. How would you determine whether the strategies you have implemented are effective?
9. How comfortable are you with your current security strategy regarding BYOD?

Conceptual Framework

I used Rogers's (1975) PMT as the foundation for my exploration of the strategies used to secure and protect data on a network where personal portable devices are permitted to connect. Rogers based the development of PMT in 1975 on three crucial components of fear appeal: the severity of an event, the likelihood of the event occurring, and the availability of a protective measure (Rogers, 1975). In 1983, Rogers modified the theory to contain the following four beliefs: the threat is serious, there is a chance that the threat may happen, a way to mitigate the threat is available, and the corrective actions are effective (Rogers, 1983). The features of PMT suggest that perception of a threat would lead to formulating a solution that then motivates a person to carry out the mitigation actions (Westcott, Ronan, Bambrick, & Taylor, 2017).

Hanus and Wu (2016) used PMT to explore how security awareness affects a home user's protective behavior towards desktop security. Dang-Pham and Pittayachawan (2015) also used PMT to investigate whether malware avoidance behavior when using one's personal device changes depending on the location of use and what factors influence malware avoidance behaviors at home and in a BYOD-enabled environment. Regarding my study, the anticipation of potential threats or risks may motivate IT security professionals to enact mitigation or prevention activities or strategies. This theory was helpful in explaining whether BYOD is a security threat from the perspective of IT security professionals and indicating the strength of the strategy based on the motivation of the individual. Figure 1 provides a visual depiction of the PMT.

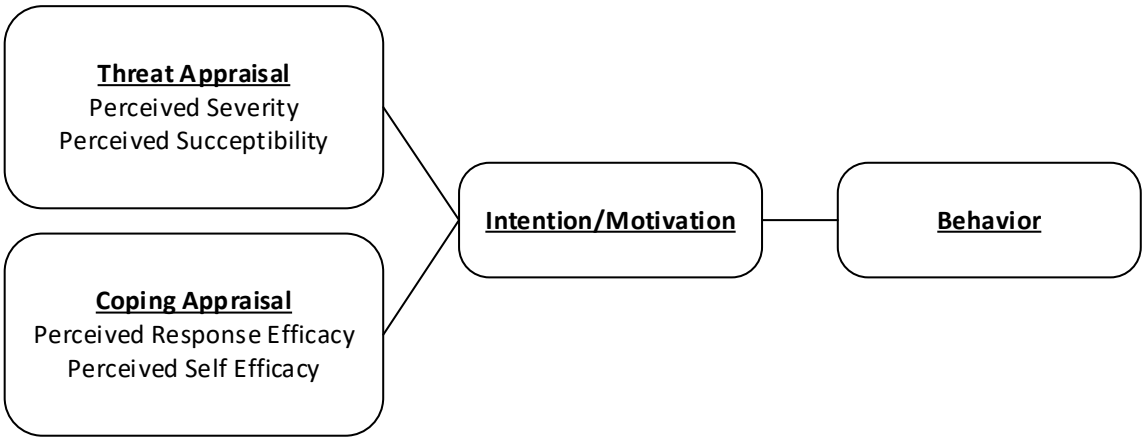

Figure 1. Visual depiction of the protection motivation theory (Rogers, 1975).

Definition of Terms

Following are the operational definitions used in this study:

Bring your own device (BYOD): The practice of companies to allow their employees to use personal mobile devices like smartphones, laptops, and tablets to access business IT resources such as applications and data (Ogie, 2016). BYOD is also known as choose your own device (CYOD), bring our own thing (BYOT), bring your own technology (BYOT), bring your own anything (BYOA), and bring your own application (BYOA; "State of Play report," 2014; Woodside & Amiri, 2014).

Information technology (IT): Technologies that generate, store, transform, and process images, text, sound, and digital information like computers, audio and video recorders, smartphones, and tablets (Zhou, 2017); or simply hardware and software for information collection, storage, processing, and presentation (Kaur, 2016).

Knowledge-attitudes-practices (KAP): A survey method that focuses on the change in knowledge, attitudes, and practices in regard to a certain topic (Liu, Chen, Solanas, & He, 2017).

Mobile devices: Items such as laptops, netbooks, e-readers, smartphones, tab devices, and similar devices (French, Guo, & Shim, 2014).

Ubiquitous: The ability to access any type of network resource from anywhere and at any time (Chen, Wang, Li, Chen, & Cai, 2019; Ghaemi Rad, Sadeghi-Niaraki, Abbasi, & Choi, 2018).

Assumptions, Limitations, and Delimitations

Assumptions

An assumption is a position or idea that has been accepted as true or taken for granted until proven otherwise (Simonson, 2016). The first assumption was that the respondents were currently managing a campus network environment that allows users to access departmental resources using their personal mobile devices. The second assumption was that the participants would provide honest answers to semistructured questions during the face-to-face interviews.

Limitations

Limitations are uncontrollable restrictions or deficiencies that may influence the outcome of an event (Alvinius, Johansson, & Larsson, 2017). The first limitation of this study was that the location of the interviews changed according to the geographic location of each campus or facility. The second limitation was that the time allotted may have limited the amount of data collected.

Delimitations

Delimitations are intentional exclusions, inclusions, and limitations imposed on the study by the researcher (Barnwell & Stone, 2016). The delimitation placed on this study included the purposive selection of 10 participants with at least two years of network security management experience of a BYOD-enabled environment in a California university.

Significance of the Study

I explored the strategies used to secure and protect the information on networks where BYOD had been adopted. University networks are more vulnerable by design compared to other business networks due to the nature of the organization; hence, cybercriminals target universities

and colleges more (Bartolacci, LeBlanc, & Podhradsky, 2014; Maimon, Kamerdze, Cukier, & Sobesto, 2013). In addition to identifying the strategies for securing a BYOD-enabled environment, I also sought to understand the IT professionals' mindset while executing the strategies.

Contribution to Information Technology Practice

This study may offer the IT community strategies and recommendations for securing a BYOD accessible network in university settings. Knowledge of these strategies may help leaders of other organizations, both inside and outside of academia, model, replicate, and implement network environments that protect and secure both organizational data and data on personal mobile devices of users. Having additional strategies to secure information and data may also reduce the spread of malicious cyber threats that may financially affect businesses and local economies.

Implications for Social Change

The positive social change that may come about because of this study would be the detection, reduction, and prevention of cyber activity by threat actors before they have a chance to obtain sensitive information that could devastate the information owners and the businesses responsible for securing the information. Having strategies in place to address security based on the results from this study may compel IT security professionals to develop, establish, or improve existing security strategies. Perhaps with an effective security strategy, both universities and users may be more at ease when devices are connected to the network or tunneling inbound through a virtual private network (VPN) connection.

A Review of the Professional and Academic Literature

The purpose of this qualitative descriptive multiple-case study was to explore the strategies IT security professionals working in a university setting use to secure an environment

to support BYOD. I performed the literature review in two parts. The first part covered the conceptual framework and the second part, the phenomenon of BYOD. I begin the literature review by discussing the conceptual framework selected for this study, PMT, and the two appraisal processes that are the basis of the framework. To provide contrast, I discuss several rival theories that I considered. The discussion about BYOD begins with an historical account, followed by discussion of its effect in the higher education environment and the strategies used to secure the threats and challenges introduced by the phenomenon.

Literature Search Strategy

Using Walden University's Thoreau multisearch database tool, I conducted a search using the search string: *security, protection motivation theory or PMT, and information technology*. To further refine the search, I limited findings to those with publication dates between 2015 and 2018 and appearing in peer-reviewed scholarly journals only. As a result, the search yielded 15 peer-reviewed journal articles regarding PMT, information technology, and security. For information regarding BYOD security in higher education, I used the Thoreau database again with the same settings but with the search string, *((BYOD or "Bring your own device") or (BYOT or "Bring your own technology")) and ("higher education" or college or universities) and (security or risk)*. The search produced 95 articles, of which 78 were confirmed as peer-reviewed sources. I identified additional articles using the Google Scholar search engine using similar key words and phrases along with a phrase in the queries to exclude theses, dissertations, and books. This literature review consists of 101 journal articles; 96% are peer-reviewed, and 87% are within 5 years of my anticipated graduation date of 2019.

Protection Motivation Theory (PMT)

Background of the protection motivation theory. Rogers (1975) initially proposed the PMT to demonstrate how stimulus variables in a fear appeal affect the decision to take action.

Based on Fishbein and Ajzen's (as cited in Tsai et al., 2016) theory of reasoned action (TRA), Rogers proposed three key components of fear appeal: the magnitude of noxiousness of a depicted event, the probability of that event's occurrence, and the efficacy of a protective response. These components are assessed and placed on dimensions of an event's appraised severity, expectancy of exposure, or belief in the efficacy of the identified coping response leading to the arousal of protection motivation resulting in the consideration of a recommended response (see Figure 2; Rogers, 1975). In this version of PMT, Rogers stated that attitude change is a function of the amount of protective motivation produced by the cognitive appraisal process and not a result of the emotion of fear.

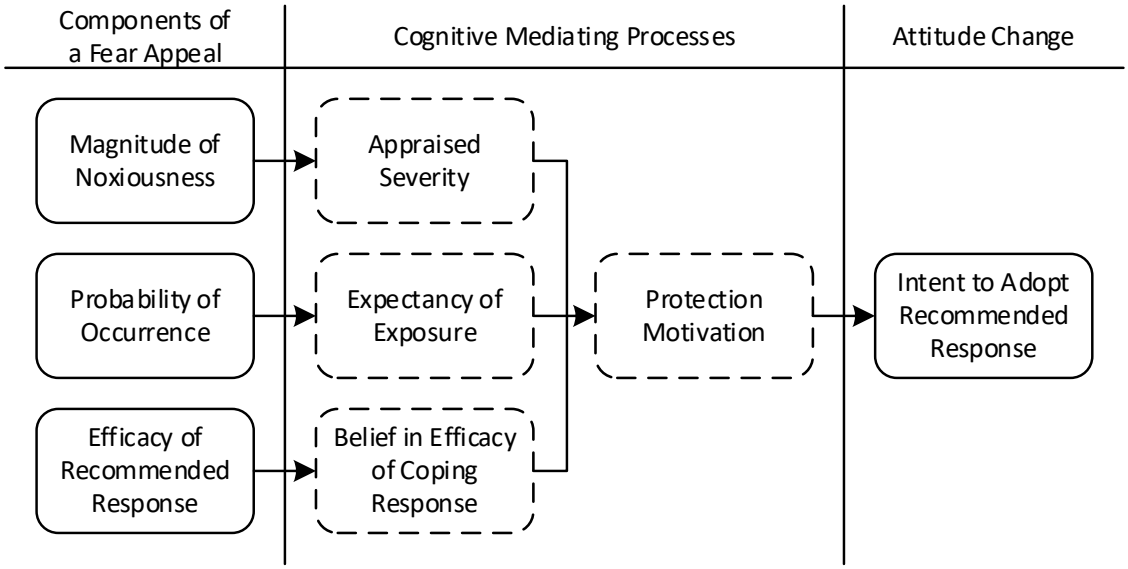

Figure 2. The protection motivation schema as expressed by Rogers (1975). Reprinted from "A Protection Motivation Theory of Fear Appeals and Attitude Change," by R. W. Rogers, 1975, *The Journal of Psychology*, *91*(1), p. 99. Copyright 2001 by Taylor & Francis Ltd. Reprinted with permission (see Appendix A).

The magnitude of noxiousness and probability of occurrence are associated with threat and translate to appraised severity and expectancy of exposure while the efficacy of

recommended responses is associated with the coping response and translates to belief in the efficacy of coping response (Makarovs & Achterberg, 2017). Bolkan and Goodboy (2016) clarified that motivation to adopt and engage in protective behaviors requires all three key components to be present. Dörnyei and Gyulavári (2016) observed that PMT explains the concept of risk and focusses attention on severity and likelihood of a negative event occurring; however; Magnan, Shorey Fennell, and Brady (2017) identified a weakness in the PMT model and pointed out that although PMT recognizes that threat induces fear, it does not specify how fear fits into the predictive equation and influences the appraisal.

The PMT has changed since its conception. Six years after the initial introduction of the PMT, Rogers (1983) presented an improved version that included a broader explanation of the information sources that would initiate the coping process, more cognitive mediating processes, and a more complete description of the coping modes while retaining the components of the original model. Rewards (either intrinsic or extrinsic) related to the threat, response costs, and self-efficacy related to behavior change were added to the original theory and believed to be important to the thought processes (Sommestad, Karlzén, & Hallberg, 2015). The sources of information--may be environmental and include verbal persuasion and observational learning or intrapersonal consisting of personality variables and prior experiences--initiate the cognitive mediating processes, threat appraisal, and coping appraisal and influence the magnitude of protection motivation affecting the decision to execute or reject a coping response (see Figure 3; Rogers, 1983). The PMT was originally developed for health-related studies; however, Clubb and Hinkle (2015) adapted the model to explain crime-related protective behavior by exploring the sources of information, threat appraisal, coping appraisal, and coping modes with the understanding that protection motivation is a summation of both the threat and coping appraisal which results in one or more of the coping modes. Other scholars have also used PMT as a

conceptual framework to explore the motivation to perform protection behavior in an information technology security context (Torten, Reaiche, & Boyle, 2018; Williams & Bamikole, 2019).

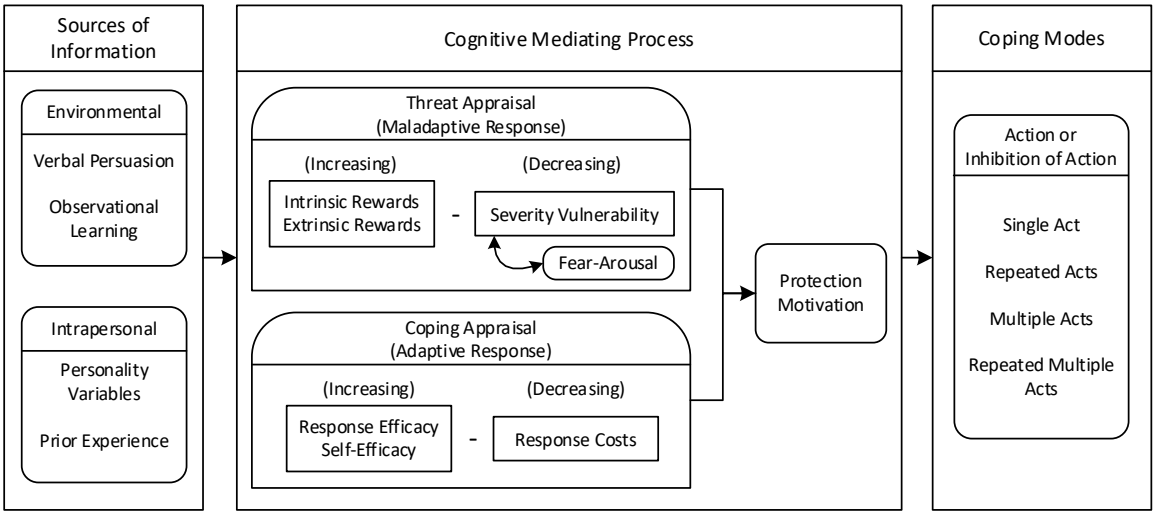

Figure 3. The protection motivation schema as expressed by Rogers (1983). Reprinted from *Social Psychophysiology: A Sourcebook* (p. 168), by R. W. Rogers, 1983, New York, NY: Guilford Publications. Copyright 1983 by Guilford Press. Reprinted with permission (see Appendix B).

Posey, Roberts, and Lowry (2015), in the context of organizational security, described the components of threat appraisal and coping appraisal where

- threat vulnerability is the feeling of susceptibility to a threat or probability of a threat occurring;
- threat severity is the perceived level of harm the threat would cause; rewards is the experience of pleasure or satisfaction from the risky behavior;
- response efficacy is the perception that the coping response is effective in addressing the threat;
- self-efficacy is the belief that the individual is fully capable of executing the prescribed coping response; and

- response costs are possible expenses, inconveniences, difficulties, and potential side effects sustained while responding to the threat.

Summation of these components leads to protection motivation, the intention or motivation to perform the coping response (Magnan et al., 2017). Furthermore, Razak, Marmaya, and Karim (2018) added that fear arousal indirectly affects attitude and behavior through the threat severity and vulnerability appraisal process. The inclusion of fear-arousal in this version of PMT addressed the concern expressed by Magnan et al. (2017) regarding the location of fear in the predictive model. Kaspar (2015) included that the perceived severity and perceived vulnerability components would reduce the chance of risky behavior while the awards would boost ongoing maladaptive behavior; likewise, self-efficacy and response efficacy increase the chance of performing the recommended protective behavior while the perceived response cost may diminish the motivation to proceed with the recommended action. The motivation to perform protective behavior may be inhibited by maladaptive rewards and response costs.

Protection motivation theory with other theories. The PMT is a versatile framework that has been extended and used in conjunction with other frameworks. Concepts from PMT have been extended to support other theories like the technology threat avoidance theory such that during the coping appraisal process, an individual may be proactive and adaptive by implementing preventative strategies (Hanus, Windsor, & Wu, 2018; Tsai et al., 2016). Chen and Zahedi (2016) conducted a cross-national comparative study of online security perceptions and behaviors of users in the United States and China by contextualizing PMT and technology threat avoidance theory through a polycontextual lens that included culture, philosophy, history, politics, economics, and technology. The results indicated that national and individual differences influence self-efficacy and perceived response efficacy leading to either avoidance or security behaviors (Chen & Zahedi, 2016). Boehmer, LaRose, Rifon, Alhabash, and Cotten (2015)

extended PMT by proposing a new explanatory variable called personal responsibility that would play a part in influencing protective behavior when combined with threat perceptions to examine the online behavior of college students concerning safety. Safa et al. (2015) and Thompson, McGill, and Wang (2017) conducted survey studies using models based on the TPB and PMT to explain and justify how information security conscious care behavior is formed and used to mitigate information security risks and to better understand actual security behavior of home computer and mobile device users, respectively. Zahedi, Abbasi, and Chen (2015) extended the core PMT constructs to include the detection tool's performance and cost of error, the users' dependence on the detection tool, and success in self-protection against cyber threats to the detection tool impact theory. Gao, Li, and Luo (2015) developed an integrated acceptance model comprised of the unified theory of acceptance and use of technology 2, PMT, and privacy calculus theory to find the driving force behind the adoption of health information technology. Gao, Li, and Luo stated that PMT is appropriate to investigate an individual's behavior towards health information technology and incorporated the concepts of response efficacy, perceived vulnerability, and perceived severity from PMT into their model. While concepts from PMT may be used to supplement other theories, in this study, PMT was exclusively used to explore the motivation underlying an IT professional performing protective behaviors in defense of the organization's networking environment where BYOD is present.

Protection motivation theory in security and privacy. There have been numerous studies where researchers enlisted PMT as the research framework or model to explore motivation and behavior within the context of cyber and information security and privacy. Even though PMT originated in health care, applications have extended to other areas of risk research like computer security (Thompson et al., 2017). Shillair et al. (2015) used PMT as the theoretical framework for their quantitative online safety intervention study to assess the value of

intervention strategies on safe online behaviors. According to Warkentin, Johnston, Shropshire, and Barnett (2016), prior research into protective security behaviors did not extend past the point of initial adoption. To address this gap in the literature, they designed a model employing PMT as the underlying theoretical framework using constructs such as perceived threat severity, perceived threat susceptibility, self-efficacy, and response efficacy to understand the factors associated with continued protective security behaviors (Warkentin et al., 2016). Jansen, Veenstra, Zuurveen, and Stol (2016) sought to explain the protective security strategies used in defense of online threats by entrepreneurs. Jiang et al. (2016) conducted qualitative focus group studies using PMT as the guiding research framework to examine how online safety was perceived, coping strategies were used, and online self-protection was performed by three different generational age groups while Jansen and Leukfeldt (2016) implemented PMT along with the routine activity approach in a qualitative multiple-case study to explore the factors resulting in online fraud victimization. Using PMT in a qualitative capacity would allow for a more in-depth understanding of the human thought process (Jiang et al., 2016). Cyber and information security threats are present wherever there is data with some intrinsic value. The PMT may be used to understand the motivation leading to protecting this data.

Inconsistencies with the protection motivation theory. Some researchers have identified anomalies when using PMT. Chen, Beaudoin, and Hong (2016) proposed a three-step privacy protection behavior model using PMT where negative privacy experiences increase the motivation factor to perform the protection behavior; however, their findings were inconsistent with their proposed model where protection motivation was bypassed and privacy experiences directly led to protection behaviors. Chen, Beaudoin, and Hong (2017) attributed the inconsistencies to possible limitations in measurement or theory and proposed two new theories built upon PMT and the extended parallel process model. Chou and Chou (2016) conducted a

quantitative survey study using PMT to explore the factors associated with risky information security behavior of 505 primary and secondary school teachers in Taiwan. Contrary to PMT, the teachers continued to exhibit risky behavior despite understanding the risks to online personal data (Chou & Chou, 2016). Similarly, Doane, Boothe, Pearson, and Kelley (2016) found that college students who engaged in risky online behavior perceived themselves to be more susceptible to cyberbullying while having few intentions to engage in protective behavior; PMT suggests that motivation to engage in safe behavior would be a result of an increased perception of vulnerability to victimization. Sommestad et al. (2015) presented a meta-analysis to evaluate how information security behavior influences the efficacy component of PMT. The results indicated that, in cases where the threat pertains to the individual and not the organization or others, PMT may explain voluntary information security behavior better than mandatory security behavior and information security behavior better with concrete or specific threats and coping methods (Sommestad et al., 2015). Thompson et al. (2017) found inconsistent results such that in determining personal computing security intentions, perceived vulnerability, self-efficacy, and response cost were important while mobile device security behaviors were only associated with perceived severity, and response efficacy was not influential in either context. All of these researchers followed a quantitative method; as such, determining the motivation to perform protection behavior may have been limited by the data collection protocol.

Protection motivation theory and BYOD. Some researchers have used PMT to explore protection motivation behavior associated with BYOD. Crossler, Long, Loraas, and Trinkle (2014) conducted a survey study of 444 participants from two large universities and college-educated white-collar workers from the general public to examine the factors that would motivate employees to comply with BYOD policies using PMT as the theoretical framework and found that contextual factors, the dependent variable choice, and the sample choice can affect the

various components of the PMT model. The results from Dang-Pham and Pittayachawan's (2015) research echoed Crossler et al.'s notion that context affects intention to perform avoidance behavior; university students were found to be more motivated to perform malware avoidance behavior at university due to a higher level of perceived vulnerability than at home. In another BYOD study, Ismail, Singh, Mustaffa, Keikhosrokiani, and Zulkefli (2017) designed a survey based on PMT to explore watering hole avoidance factors. Verkijika (2018) conducted a quantitative study to understand the security behaviors of smartphone users in South Africa using a modified version of PMT that includes the role of anticipated regret. While maladaptive rewards correspond to hedonic satisfaction from continuing a risky behavior, anticipated regret would take its place in the threat appraisal process as the potential remorse from the anticipated outcome of continuing or not continuing the risky activity (Verkijika, 2018). Using PMT together with the qualitative methodology allows for a deeper understanding of the motivation to manage a secure network environment with BYOD.

Analysis of Rival Theories

Knowledge, attitudes, and practice (KAP). What people know, feel, and behave towards a certain topic may be obtained from KAP studies (Abdullah, Ismail, Nor, & Wahab, 2014). The origin and history of knowledge-attitude-practice (KAP) survey is unclear. The earliest reference of KAP use was in a dental health study in a Denver Public Schools system in the mid-1940s where the purpose of the study was to collect information about the knowledge, attitudes, and practices related to dental health from resident pupils in school systems with differing dental health education approaches (Myers & Downs, 1968). In 1965, the KAP survey was also used to measure the level and changes in married women's knowledge about, attitude toward, and practice of family planning (Chow, 1968). Although the origins of KAP is unclear,

researchers continue to use the tool to gauge what people know, what their views are towards a particular topic, and what they do concerning the topic.

The KAP data may not be completely accurate due to the collection method which may lead to inconsistent results. Data collected in the KAP study were self-reported and not based on observations (Kossover-Smith et al., 2017). According to Genga, Achieng, Njiri, and Ezzi (2017), limitations of using a KAP survey method may involve participants not providing fully honest answers but responding with socially desired responses. Alavi, Dabbagh, Abbasi, and Mehrdad (2017) designed a cross-sectional study to evaluate the radiation protection (RP) knowledge, attitude, and compliance to practice self-protection against radiation and indicated that the study was a "self-reported questionnaire-based study and the accuracy of the answers may not be seen in participants' practice" which was in line with Kossover-Smith et al. (2017) and Genga et al.'s (2017) findings. Although the questionnaire is self-administered and self-reported, and actual behavior may not be accurately reported, beliefs and knowledge can still be measured while eliminating the researcher as a source of bias (Singhal, Acharya, & Thakur, 2017). As an example, Mazloomy et al. (2014) conducted a descriptive cross-sectional study of 200 women referred to health centers in Yazd to understand their position on cardiovascular diseases and risks using KAP and discovered that the knowledge and practice scores were low but attitude was high; attitude did not result in practice although 91 percent of the participants had indicated interest in exercise but 26 percent reported exercising three times per week. The participants in this study may have wanted or intended to exercise but in reality, did not engage in the activity.

The relationship between high attitude and low practice may be observed in other unrelated studies. Liu et al. (2017) designed and conducted a KAP survey among municipal hospitals in Wuxi, China to find out how much the respondents knew about the Internet of Things (IoT), their attitude and openness to using IoT devices in health care, and the current level of IoT

implementation in their hospitals. Liu et al. revealed that regarding knowledge and attitudes, all respondents agreed on the user-definition of Internet of Things (IoT) and that it would improve effectiveness of health-care services but the cost of implementation and other factors would act as a blocker but when it came to practice, five respondents attested to using the technology for tracking but were actually not used. Daneshkohan, Hosseinzadeh, Abolfathi, Hekmatifar, and Bajalanlou (2015) determined that most students in Shahid Beheshti School of Health had poor knowledge and practice of Internet search but still possessed a positive attitude towards using the Internet for learning. Self-administered or self-reported KAP surveys may not elicit truthful or honest responses from participants regarding attitude and practice and do not capture or measure motivation between the two components.

Love and Tuokko (2016) mentioned that even though KAP surveys are self-reported and social desirability could influence the responses, ensuring anonymity and confidentiality, as in using an online survey, may address the issue. Employing an online survey may improve the quality of the responses from participants but as de Bont, Francis, Dinant, and Cals, (2014) point out, “Internet-based questionnaire may have introduced selection bias, as only Internet users were able to participate in the study.” Since the KAP survey is a self-administered questionnaire, the ability to ask follow-up questions to gain deeper understanding and meaning is unlikely, KAP would not be appropriate for this study.

The relationship between the KAP components exists where attitudes and practices may be achieved by increasing the knowledge component (Sambo et al., 2014). Sambo et al. (2014) stated that KAP studies have been globally utilized in the public health industry to identify knowledge gaps, beliefs and behavior patterns that may inhibit desired behavior. Memon et al. (2014) conducted an observational cross-sectional study to assess the KAP towards diabetes and diabetes retinopathy in Bin Qasim and found knowledge gaps and low attitude and practice

among the female, illiterate, and non-diabetic participants resulting in suggestions for audiovisual awareness and educational material. Increasing the knowledge component was often the solution to improving attitude and practice.

Education was almost always the recommended course of action in KAP studies. Farooqui, Yahaya, Hussien, and Farooqui (2016) conducted a cross-sectional KAP study in Malaysia regarding blood donations among health care workers and found the knowledge, attitude, and practice levels to be low and recommended education and motivation through information dissemination campaigns. Similarly, Kebede, Retta, Abuye, and Malde (2016) conducted focus group discussions to collect knowledge, attitude, and practice information from communities in Ethiopia exposed to fluoride contamination and fluorosis to develop coping strategies, and the results indicated that there was a gap in knowledge and misconceptions regarding fluoride and its effects. However, the participants' attitude towards efforts to provide safe water for the community was positive (Kebede et al., 2016). Kebede et al. suggested educating the community regarding health and nutrition would reduce the risks associated with ingesting fluoride until a more permanent solution is in place. Niroomand et al. (2016) conducted a multicenter analytical cross-sectional study in Iran to evaluate the KAP level of type-2 diabetic patients regarding diabetes and found a positive correlation between duration of diabetic infliction and KAP level which supports providing diabetic education to newly diagnosed patients before complications occur.

Providing education and training may or may not result in the desired outcome. Madhwani and Nag (2017) conducted a web-based KAP intervention study on 203 employees in a multinational corporation to explore the effectiveness of cost-effective methods of disseminating information leading to an improvement in practice behavior to prevent musculoskeletal discomfort. The results indicated that the intervention was successful in

modifying behavior towards maintaining healthy body posture. However, Yin et al. (2017) were not as fortunate when they conducted a cross-sectional and intervention KAP study with the understanding that knowledge and information would influence positive attitude and belief resulting in change in practice. Instead of seeing an improvement in practice, no statistical improvement was observed even though there was an increase in knowledge and attitude (Yin et al., 2017). Increasing knowledge may not be the only factor for improving attitude and practice. Khan, Sarriff, Khan, and Mallhi (2014) found that participants with a higher chance of being affected by an affliction may have more knowledge, attitude, and practice towards that affliction.

The KAP measurements may be imprecise or misleading. Li et al. (2015) collected KAP information from Tibetan communities regarding cystic echinococcosis and the measurement of attitude was flawed due to misconstructed questions like "[d]id you have a medical check-up recently?" and the choices were "[b]y ultrasound", "[b]lood test", and "[d]on't know" when the logical answers should have been "yes", "no", or "don't know". This notion was not limited to attitude, practice was also inadequately measured as demonstrated in Kattoor, Thomas, Abraham, Bahia, and Kenchaiah,'s (2017) tobacco cessation study where impedance to practice was attributed to lack of interest among patients, shortage of time, and limited resources which were outside the control of the participants.

The KAP approach is useful in identifying training opportunities that may affect practice but does not address the motivation to execute the desired security behavior. Xiao et al. (2014) posited that PMT may be an extension to KAP for addressing cognitive risk appraisal and benefits from performing protective strategies. Furthermore, their findings revealed that both the threat and coping appeal pathways of PMT are related to intentions to perform protective behaviors (Xiao et al., 2014). The notion that PMT may have been conceived by KAP may be presumptuous considering the relationship between PMT and TPB.

Theory of planned behavior (TPB). The TPB and PMT share the same origin. The theory of planned behavior is a modification of TRA that considers perceived and actual control of the considered behavior rather than looking at intentions to perform or not perform a behavior as a predictor or determinant of the action; however, it does not explain behavior stimulated by health threats (Ajzen, 1985; Rogers, 1975). Luor, Lu, Yu, and Lu (2015) presented that both TRA and TPB consider that attitude is the first antecedent of behavior intention and behavior intention is the antecedent of actual behavior. The TPB is comprised of five constructs: attitude, normative beliefs, self-efficacy or intentions, perceived behavioral control, and behavior (Foltz, Newkirk, & Schwager, 2016; Rocha Flores & Ekstedt, 2016). Ajzen (1985) stated that the relationship between behavioral expectation and actual behavior is dependent on the perceived control and actual control over the intended behavior whereby TPB is relevant when control is limited and the probability of failure is high. Rocha Flores and Ekstedt (2016) clarified that the core principle of TPB is the intention to perform a target behavior and the successful execution of the behavior relies on the strength of the intention. Badran, Pluye, and Grad (2015) reduced the five constructs of TPB down to three constructs--knowledge, attitude, and behavior--to understand family physicians' perception of, and the advantaged and disadvantages of educational e-mail in a qualitative descriptive study. Behavioral intentions resulting in actual behavior may be predicted using three TPB factors: attitude toward the behavior, subjective norms, and perceived behavioral control (Bélanger, Collignon, Enget, & Negangard, 2017; Chu, Chau, & So, 2015; Safa & Von Solms, 2016). Jafarkarimi, Saadatdoost, Sim, and Hee (2016) employ the aforementioned TPB factors along with personal normative beliefs, moral intensity, and perceived threat of legal punishment to predict behavioral intent to use social networking sites (SNSs) in unethical ways. Kim and Kim (2017) substituted compliance behavioral belief, social pressure, and compliance knowledge for each of the factors respectively in their study. Arpaci, Kilicer, and Bardakci (2015)

proposed that specific situational beliefs precede attitude; however, beliefs in one situation may not be relevant in other situations. In determining intention, each of the constructs is conceptually independent of each other (Bélanger et al., 2017). In short, the constructs of TPB independently influences behavioral expectation and actual behavior.

The TPB is adaptable. The number of TPB constructs has been extended, as in Foltz et al.'s (2016) study where apathy and social trust were added, and reduced by exclusion, as in Inauen and Mosler's (2016) study where only attitude, descriptive norms, and intentions were considered. However; regarding motivation to perform a behavior, TPB was designed to predict behavior by looking at attitude, perceived behavioral control, and subjective norms but not the motivation to engage in a specific behavior (Safa & Von Solms, 2016). To include motivation, TPB needed to be combined with other theories like the motivation theory (Safa & Von Solms, 2016). Bélanger et al. (2017) integrated perceived threat severity and perceived threat vulnerability from PMT as direct determinants of attitude which affects intention. However, Kim and Kim (2017) assumed, tested, and concluded that behavioral intention was influenced by compliance knowledge or perceived behavioral control which is affected by belief or attitude and social pressure or subjective norms. This differs from the original TPB, thus presenting a discrepancy that warrants attention in future research.

The TPB has been noted as having flaws. Chu et al. (2015) indicated that TPB was ineffective in predicting risky behavior probably due to not accounting for the decision-making process leading up to risky behavior. They proposed incorporating a dual-process approach with TPB to explain the information system misuse by employees.

In the context of information security, a unified model that integrates multiple theories into one have been proposed. Moody, Siponen, and Pahnila (2018) proposed a unified model of information security policy compliance (UMISPC) that combines 11 theories into one inclusive

theory. Cram, Proudfoot, and D'Arcy (2017) suggested that a complementary approach that simultaneously considers different theories but through separate lenses, like how deterrence theory, PMT, and TPB have been used to understand the relationship between the organization and individual employees on policy compliance, may provide new insights of a phenomenon from different perspectives. Although having one all-inclusive theory for information security may seem efficient and convenient, the additional components may be more than what is needed in this study. Using one theoretical lens may prove more beneficial to future studies on similar topics.

Bring Your Own Device (BYOD)

A brief history of BYOD. The BYOD phenomenon is also known by other names: bring your own technology (BYOT), bring your own phone (BYOP), or bring your own personal computer (BYOPC) (Tchao, Ansah, & Kotey, 2017). BYOD initially referred to cell phones but evolved to include personal electronic devices like smartphones, tablets, and laptops with the capabilities to connect to the corporate network (Utter & Rea, 2015). In the corporate or business environment, BYOD is the alternative to corporate-owned, personally enabled (COPE) device use scenarios (Oluwatimi, Midi, & Bertino, 2017). Simply put, any personal mobile or portable devices permitted to connect to the corporate network so that the employee may perform business-related tasks is considered a BYOD device. In 2009, Intel's senior leadership noticed that employees were bringing their personal devices in and connecting to the network to do work but instead of ending the new practice, the company allowed employees to continue since it led to improved productivity and lowered costs (Burns-Sardone, 2014). Cheng, Guan, and Chau (2016) clarified that the employees' devices included laptops, smartphones, and tablet PCs. While Burns-Sardone (2014) and Cheng et al. (2016) agreed that the employees willingly brought in their own devices and started the movement, Deng, Ma, and Li (2016) expressed that the employees were

expected to bring in their devices and connect to the network. Additional advantages to BYOD include increased employee morale and job satisfaction by allowing employees the freedom to purchase devices that they prefer, the cost due to theft is reduced because employees are more vigilant in preventing loss of their own the devices, and only one device may be carried around instead of two; thus providing flexibility to and productivity from employees (Sebescen & Vitak, 2017; Smith, 2017). Cho and Ip (2018) suggested that organizations may stimulate BYOD adoption through educating and empowering employees leading to increased productivity and loyalty. Most researchers and authors agree that BYOD came out of Intel but Garba, Armarego, and Murray (2015) believe that BYOD was first embraced by Cisco in the same year, 2009. Regardless of the true origins, BYOD is now commonly practiced in many organizations; however, balancing risks and benefits is a challenge (Sebescen & Vitak, 2017; Tchao et al., 2017).

Risks and vulnerabilities of BYOD. The use of BYOD invites malicious cyber-attacks. Advanced persistent threats (APT) like the watering hole and malware affects higher education as well as private businesses and individuals (Dang-Pham & Pittayachawan, 2015; Ismail et al., 2017). The APT attacks may result in loss of intellectual property, sensitive and confidential information, and customer records through the use of social engineering and exploitation of vulnerabilities (Bann, Singh, & Samsudin, 2015). Bann et al. (2015) identified the key features of APT as: (a) *targeted* – focused and selective of victims and goals, (b) *advanced* – comprised of multiple techniques including custom code to gain access to vulnerable networks and devices, (c) *persistent* – the attack may span a long period of time in which information is leaked without being detected, and (d) *evasive* – capable of circumventing network security strategies like firewalls and intrusion prevention systems (IPS). In 2017, at least 150 universities were targets of the Wannacry ransomware (Mohurle & Patil, 2017). The infections not only affect

the BYOD device but may quickly spread to other devices on the network (Singh, Chan, & Zulkefli, 2017). Additional concerns include confidentially and privacy risks to the businesses that have adopted BYOD (Vorakulpipat, Sirapaisan, Rattanalerdnusorn, & Savangsuk, 2017). The businesses may not have control over the applications and the devices may not be protected from malware, increasing the risk of data breach (Oluwatimi et al., 2017).

By introducing BYOD, businesses' proprietary information is vulnerable to being copied, modified, or deleted from personally owned devices by both internal and external actors (Smith, 2017). The malware and viruses may be accidentally installed when a user clicks on a link in a phishing e-mail or application download; devices connected to unsecured networks are vulnerable to attacks like Wi-Fi hijacking, bluejacking, and bluesnarfing; and while connected to the network, BYOD devices may contain credentials that may provide access to services or sensitive company and personal data (Singh et al., 2017; Wanja, 2018). A user's private and personal information may be exposed or shared with the employer, presenting a privacy concern (Smith, 2017). Bello, Murray, and Armarego (2017) identified the absence of policies, lack of security controls, lack of security awareness, and lack of privacy as risks and concerns associated with BYOD adoption. The security and privacy threats that affect the organization also affect the users.

Education and BYOD. Primary schools have been incorporating BYOD as a learning enhancement strategy and institutions of higher education have started adopting BYOD practices. Hung (2017) found that students in a flipped learning model welcomed the use of their personal mobile devices as interaction tools, used in the place of clickers, but expressed concerns over the reliability of the wireless network connection. While having the potential to improve learning, BYOD may also be a source of distraction when lessons are not interesting or engaging to keep the student's focus (Kay, Benzimra, & Li, 2017). In a quasi-experimental pretest and posttest

control group design study to investigate the effects of incorporating BYOD in language learning, Chou, Chang, and Lin (2017) reported that students in the traditional instruction class performed better than the students in the BYOD class on the pretest and posttest; however, on the delayed posttest administered one month after the posttest, there were no noticeable differences in the test results except for better knowledge retention and positive attitudes towards BYOD by students in the BYOD class.

Song (2016) conducted a mixed-methods study to investigate the science inquiry skills development of students in a Hong Kong primary school and found that students in a BYOD-supported learning environment obtained deeper understanding while enjoying the learning process. Song and Kong (2017) conducted a qualitative study to examine the educational implications of BYOD in higher education from the teacher's perspective and identified seven affordances and three constraints for the use of BYOD as a pedogeological tool. The results from Song and Kong's study indicated that the teachers' perception towards the adoption of BYOD in teaching varied. Dang-Pham and Pittayachawan (2015) conducted a survey study to explain the change in student malware avoidance intentions when at home and at a BYOD-enabled university in Australia and revealed that although students in the study were cautious when checking e-mails and browsing websites both at home and at university, they were more inclined to demonstrate malware-avoidance behavior in the home context than in the university context. Singh et al. (2017) conducted a similar study involving students from a higher education institution in Malaysia to investigate their security and privacy awareness and confirmed that the BYOD trend was indeed spreading into higher education and that the students possessed a basic security and privacy awareness and knowledge of mobile devices but were concerned about the mobile data security controls. Though most studies show some level of BYOD acceptance in higher education, Gillies (2016) reported that despite the benefits to the faculty and students, the attitude

towards mobile phones, historical use of the personal device, equity of access, and unclear control and governance were perceived as barriers to the adoption of BYOD at one institution of higher education in the United Kingdom.

The inclusion of BYOD in education is not limited to classroom learning. Brouwer, Heck, and Smit (2016) presented the use of BYOD by second-year university students for mathematical study in an online learning environment, however, the digital examination rooms at the university were inadequate to accommodate the personal devices for testing. While blended learning, a mixture of online and face-to-face learning, is an emerging trend, so is the collection of data on student learning and activities and BYOD (Skiba, 2016). As educators attempt to incorporate BYOD technology into their teaching strategies, mobile security is a great concern (Spangler, Rodi, & Kiernan, 2016). Bass and Movahed (2018) revealed that BYOD improves students' participation, flexibility, and integration within the classroom by eliminating the need for switching between different equipment to conduct work. Bass and Movahed also noted that students felt that opportunities to utilize BYOD were lacking and that an increase integration of mobile learning was desired.

Strategies to mitigate BYOD-associated risks. Organizations that plan to adopt or have adopted BYOD must have some type of strategy to secure and protect data. Balboni, Berman, and Korsten (2015) prescribed that organizations need a centralized strategy to manage and secure the various device platforms brought about by the growing popularity of BYOD. Vorakulpipat et al. (2017) proposed a BYOD security framework and concluded that organizations must first clearly define the extent of support for BYOD use by developing then implementing BYOD policies that are based on the information security policies. Bello et al. (2017) also recommended that organizations develop and deploy effective BYOD management and policies that not only address security but also privacy. Smith (2017) stated that policies are

important starting points but may not account for every possible situation due to emerging technology. Additionally, Sebescen and Vitak (2017) found that employees may be complacent over time and less cautious about their actions, and compliance to the security policies do not imply that the employees understand the security policy; hence, having a security policy alone may not be effective in directing human behavior and introducing education-based training may improve employee knowledge and awareness levels resulting in more informed compliance to security policies. The use of containerization or compartmentalization of resources to isolate personal data from enterprise data using security strategies like authentication, encryption, and isolation of data and environment coupled with implementing mobile device management (MDM), mobile application management (MAM), and mobile content management (MCM) solutions may help minimize data privacy and security loss due to overlapping use in work and non-work environments (Oluwatimi et al., 2017; Smith, 2017; Spangler et al., 2016). Wanja (2018) proposed a security threat matrix, a security self-assessment tool, that would be used in conjunction with existing information and communication technology (ICT) policy to identify potential security attack risks. Bann et al. (2015) suggested employing the access control policy tool (ACPT) developed by the National Institute of Standards and Technology (NIST) and North Carolina University to deal with APT attacks and implement a mandatory access control (MAC) security policy to specifically mitigate spear-phishing attacks in a BYOD environment.

Nagios, Nessus, Wireshark, FireEye, Palo Alto firewalls, and Proofpoint Protection Server, Symantec Endpoint Protection, Malwarebytes, and NetBotz cameras are some strategic security tool used to monitor the network and infrastructure, scan and assess system vulnerabilities and flaws, capture network packets and analyze network protocols, detect and prevent threats, control the flow of inbound and outbound network traffic, filter and control e-mail-based threats, centrally manage the antivirus software, detect and remove malware, and

monitor data center activities and environmental variables (Raisinghani, 2016). Sebescen and Vitak (2017) stipulated that by implementing screen locking mechanisms, applying security updates, segregating corporate and personal data on the devices, and securing connections made through unsecured public Wi-Fi, security and privacy risks may be reduced. To address the growing BYOD use in institutions of higher learning, governance policies, malware detection, and Terms of Service (TOS) agreements were needed; however, having these tools and practices in place does not guarantee immunity to security threats (Spangler et al., 2016). Some universities may have a mobile device policy in place but the penalty for violating policy might not be serious enough. Consequences for violating policy may be a ticket, an incident report, or no punishment or sanctions at all (Misenheimer, 2016). Wanja (2018) recommends regular reviews of the university ICT security policy, vulnerability scans, penetration tests, and security audits be performed to mitigate new security threats while Akeju, Butakov, and Aghili (2018) recommended implementing good practices based on NIST special publication 800-53A RA, SANS Institute: Critical Security Controls, International Professional Practices Framework (IPPF), and ISACA Cybersecurity Nexus to protect mobile and embedded devices.

University Network Security Challenges

College and universities are higher education institutions where most people go to continue their education to meet parental expectations; to develop and harness valuable life and business skills; or to satisfy an insatiable hunger or thirst for knowledge. These institutions often foster and encourage the pursuit of knowledge and understanding by providing an environment where professors and students are free to study, learn, teach and use knowledge (Abegglen, Burns, & Sinfield, 2016; Spronken-Smith, Buissink-Smith, Bond, & Grigg, 2015). The freedom to explore and inquire by faculty and students without censorship in a college or university setting is known as academic freedom (Curnalia & Mermer, 2018; Woods et al., 2016). Woods et al.

(2016) pointed out that some faculty members interpret academic freedom as the poetic license to do whatever they want; however, the scope of academic freedom is neither limitless nor boundless. Unhindered access to information and knowledge with uncensored or unrestricted access to and from the Internet may be an invitation for unwanted cyber threats.

Academic freedom coupled with the Internet as a learning medium changes the learning landscape. Gutiérrez-Porlán, Román-García, and Sánchez-Vera (2018) found that some university students consider online communication and social networking as necessities they cannot do without. Misenheimer (2016) reported that academic freedom provided more computing freedom since content filtering was not conducted due to the need to access sites that may be considered inappropriate. The network environment at higher education institutions enables students and faculty to freely embrace pedagogy but the higher educational institutions must also consider the potential security risks associated with Internet use.

At the K-12 school level, Akeju et al. (2018) identified eight categories of risk associated with BYOD and IoT:

- network access control risks – devices are permitted to connect to the schools' wireless network without checking for threats and implementing user-side security strategies;
- end-user device risks – the devices may be lost or stolen, or its security may be compromised or misconfigured risks;
- cloud or storage risks – cloud services may serve as gateways for network security breaches;
- information privacy risks – students' online activity may be collected without the students' knowledge or consent;
- malware risks – malicious code or programs may be moved to the schools' network;

- application risks – the schools may not have control over the applications downloaded and installed;
- IoT vulnerability management – IoT devices lack or have weak security protection; and
- policy and procedure violation risks – students intentionally circumventing security restrictions and policies to allow free use of their devices.

These risks may expand past the K-12 school level and extend into the realm of higher education. Monitoring network activity was suggested as a strategy for securing a BYOD-enabled environment, however, introducing a monitoring mechanism may offset the perceived benefits of BYOD by infringing on the privacy of the employees (Lee, Warkentin, Crossler, & Otondo, 2017). Higher educational institutions are now adopting BYOD and opening their networks to new security and privacy risks.

In summary, the use of Rogers' (1983) version of PMT has been minimal with regards to qualitative studies involving information technology and even less with BYOD. The PMT has been used in combination with other theories like technology threat avoidance theory and TPB. Although inconsistencies have been observed where protection motivation was bypassed (Chen et al., 2016), risky behavior continued despite understanding the risks (Chou & Chou, 2016), and response efficacy was noninfluential in two different contexts (Thompson et al., 2017), PMT includes the decision-making process that TPB lacks and the motivation leading to the behavior that KAP lacks making it the best framework for this study.

The phenomenon where personal devices like smartphones, tablets, and laptops are permitted to connect to the corporate network to engage in work activities is known as BYOD (Utter & Rea, 2015). There are advantages and disadvantages to both the corporations and the users. Corporations that have adopted BYOD benefited from deceased cost of equipment

purchase and maintenance while increasing employee morale but expose the network to potential risk and have little control over the devices while employees and users participating in the BYOD program carry and use one device instead of two, use their own devices (Sebescen & Vitak, 2017; Smith, 2017).

The use of personal mobile devices to access work-related resources has extended past the boundaries of private corporations and into the public education sector. The use of BYOD in classroom instruction may enhance learning retention as well as being a distraction (Chou et al., 2017; Kay et al., 2017). At institutions of higher learning, students, faculty, and staff are beginning to connect personal devices to the school's network to access university resources but without the same restrictions found in private organizations. While security frameworks, policies, and tools exist, the ability to implement these strategies is diminished by academic freedom poses a security challenge. Current literature examined BYOD in higher education from the teacher, student, and administrative perspective but there has not been any inquiry from the lens of a security professional responsible for managing a university network environment. The PMT was used as the framework where the protection motivation of the security professional and the strategies employed for securing a network with BYOD devices were revealed by exploring the sources of information, threat appraisal, coping appraisal, and coping mode.

Transition and Summary

In Section 1, the background of how BYOD is an issue was presented followed by the identification of the general and specific IT problems related to BYOD. The purpose was to explore strategies from the perspective of the IT professional and the compulsion to exercise security enabling behavior to secure and manage an environment where BYOD was enabled. The nature of the study, overarching research question, and the conceptual framework were presented. For the conceptual framework, I selected the PMT to delve into the behavioral context of the IT

professional. I provide more information on the theory and the rival theories; KAP) and the TPB, in the literature review before discussing BYOD's beginning, use in higher education, and known strategies.

Section 2 provides details regarding the role of the researcher, the participant pool, how the study was designed, how the sample was determined, and how the data was collected, analyzed, and validated. Section 3 provides an overview of the study by presenting the findings of the data after being collected, analyzed and validated followed by how the study applies to professional use and affects social change. Recommendations are made for action and further study then completed with reflections and conclusions.

Section 2: The Project

Purpose Statement

The purpose of this qualitative descriptive multiple-case study is to explore the strategies IT security professionals working in a university setting use to secure an environment to support BYOD in a university system. The research population consisted of IT security professionals from UC campuses currently managing a network environment for at least two years where BYOD has been implemented. The results of this study may contribute to positive social change by highlighting strategies for securing a network to support BYOD in institutions of higher education; using these strategies, IT professionals may be better able to protect the security and privacy of personal and sensitive data on the personal devices of students, faculty, and staff and on-campus servers while connected to the institution's network. The findings of this research may be generalized to IT security practitioners in other business sectors and industries seeking to implement security on networks with BYOD devices. Also, by identifying strategies that IT security professionals may employ to secure and protect their environment, the study may lead to positive social change through the deflection of malicious intrusion attempts by external bad actors and the continued safety of sensitive and private data.

Role of the Researcher

In qualitative case study research, the researcher is the primary data collection instrument who directly observes and interviews the participants (Amri, Tahir, & Ahmad, 2017; Njaramba, Whitehouse, & Lee-Ross, 2018). The traits of a qualitative study method include sensitivity to the natural environment, the researcher taking on a participatory role in the holistic experience, the use of different perspectives, a design that is flexible and open to change, and the use of an inductive approach for data analysis (Arseven & Arseven, 2014). In this descriptive qualitative multiple-case study, I was the primary data collection instrument. I also designed the study;

developed the interview questions; selected the participants; and organized, analyzed and interpreted the data.

When the researcher is the primary data collection instrument, full disclosure is necessary. The researcher's worldview may influence and inform the research design and outcome; therefore, personal values, assumptions, and biases need to be clearly identified early in the study (Njaramba et al., 2018). I am an IT professional with over 20 years of system and server administration experience. Currently, I am in a leadership position at a university that does not have a BYOD policy. Although my role is not specific to security, I do consider data security and privacy important and an integral part of my job description. I am a functional manager which means that in addition to overseeing staff productivity, I am also responsible for certain IT tasks like server, firewall, and database maintenance and security. This study is significant due to the introduction and adoption of BYOD in institutions of higher education. In the UC system there are multiple campuses, and each campus has multiple departments where the IT management and support are decentralized. Because I work within the system, I excluded network security professionals from the campus where I am affiliated and selected participants from different campuses. Embedding reflectivity and reflexivity into a study may improve the quality of the research and mitigate researcher biases (Halcomb & Peters, 2016; Teusner, 2016). By being self-aware and discussing my personal background and relationship with the participants, consistent with the concepts of *reflectivity* and *reflexivity*, I am disclosing biases that may potentially influence the results of the study so that I may take the appropriate steps to contain and prevent data contamination due to my predispositions as much as I can.

To ensure trustworthy data and mitigate researcher biases, I similarly used triangulation by interviewing multiple participants, collecting information from documents, and member checking by confirming my interpretations of the data with the interviewees for agreement and

accuracy. Razzaghi and Afshar (2016) conducted a qualitative study to establish a physician-patient relationship model and used triangulation, peer review, and member checking to ensure data quality. A semistructured interview is a qualitative data collection method that allows the researcher to ask follow-up questions and participants to elaborate beyond the predefined questions for more in-depth responses (Bas & Kivilcim, 2017). I conducted interviews using a semistructured interview technique with open-ended questions and probing for richer and more complete responses.

I also considered the participants' well-being and the ethical issues involving human subjects. The *Belmont Report* presents an analytical framework based on three ethical principles to guide research involving human subjects: (a) *respect for persons* where researchers treat participants as autonomous agents capable of making decisions and give weight to those decisions while providing protection to those without the facilities to do so; (b) *beneficence*, which is understood as acts of kindness or charity and involves an obligation and promise to secure the well-being of the participant through doing no harm, and maximizing benefits while minimizing harms; and (c) *justice*, which involves treating participants equally and fairly accounting for the need, effort, societal contribution, and merit of each individual (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1978; see also Stellefson, Paige, Alber, Barry, & James, 2015). Adhering to the *Belmont Report* ensured that no harm came to the participants because of their participation in the study. I obtained voluntary informed consent from the participants, protected their privacy by shielding their identity and storing the data collected in a secure location to be destroyed after 5 years, and ensured that every participant received the same level of attention without prejudice.

Realizing and identifying influential factors such as biases in research is important for truthful and honest reporting. Arentz (2018) stated that researchers must be transparent and

mitigate potential and actual biases to instill truth and trust in the study and the results. To mitigate potential biases, I selected participants from other campuses and excluded my own campus. I also did not contact or discuss the topic of BYOD with any of the potential participants prior to IRB approval. Of note, the department that I work in does not currently permit BYOD.

Participants

To obtain meaningful and relevant data, care must be observed when selecting participants. Ball, Hoek, Tautolo, and Gifford (2017) selected participants based on seniority, expertise, diversity of roles, ethnicity, and political alignment. Brands and Elam (2017) selected participants who were best qualified and had direct experience in their field. Satalkar, Elger, and Shaw (2016) drew on the experienced and opinions of the participants. Participants in Satalkar et al.'s study must have met the following eligibility criteria: (a) work in a department on one of the 10 UC campuses, (b) have at least two years of experience managing a BYOD-supported network environment from a security perspective, and (c) the number of BYOD users in the environment must be greater than or equal to 50 users. Security professionals with BYOD experience may have strategies that are different from those of security professionals who manage a network environment that has not adopted BYOD.

Participants may be accessed in several ways. Kodadek et al. (2016) directly identified potential participants and then contacted them by e-mail; Mourtada, Schlecht, and DeJong (2017) enlisted the aid of a research assistant to identify the potential participants then contacted them by telephone and text messaging; and Lysaght, Krupa, Kranenburg, and Armstrong (2016), after identifying participants and confirming that they met the inclusion criteria, extended invitations to them to participate in the study electronically or through the postal service. Each year, each UC campus takes a turn in hosting different IT security conferences like the Information Security Symposium, the University of California Computing Services Conference, and the UC

Cybersecurity Summit. I reached out to the planning committee of the UC Cybersecurity Summit committee, but they were unable to lend assistance, and committees for the other conferences had not been established; therefore, additional support to recruit participants through the various planning committees was unsuccessful. I originally approached a member of the IT security group from my campus to assist with the recruiting process and the individual agreed to help; however, due to personal reasons, the individual was unable to proceed but directed me to a list of chief information security officers (CISOs) for each of the campuses that I could use to solicit support in identifying potential research participants.

Establishing a positive working relationship with the participant is crucial to gathering truthful and meaningful data. Henson (2017) stated that creating a trusting relationship through transparency will allow participants to comfortably express their opinions. Participants may be more open to sharing during the interview when active-listening is used to build trust, rapport, and understanding (Bell, Phoenix, Lovell, & Wheeler, 2015). Cebrián (2017) suggested that rapport and trust between the participant and the researcher may be promoted using semistructured interviews. To ease the participant's concern and be transparent, I made it clear that participation was completely voluntary, and the participant may withdraw at any time for any reason. During the interview, I directed my full attention and actively engage with the participant to secure trust and stimulate rapport.

Research Method and Design

The goal of this study is to explore the strategies employed by IT security professionals to secure a university network that allows the use of BYOD using a qualitative descriptive multiple-case study approach.

Method

I used a qualitative research method to explore the strategies used by security professionals to support a BYOD-enabled network environment. Using a qualitative approach, researchers may extract patterns and themes from the content-rich responses received from the participants (Bennett, Dawson, Bearman, Molloy, & Boud, 2017). Theoretical and empirical data may also be attained through a qualitative method (Najjar & Fares, 2017). Giedraitis, Stašys, and Skirpstaitė (2017) stated that a qualitative method allows the researcher to focus and gather complete data from the participants' perspective and real-life experience in addition to exploring the subjective understanding of the study topic. Data in a qualitative study may be obtained from oral communications or observations then transcribed into text and analyzed for patterns and meaning (Gibson, 2016). The qualitative research method is more suitable for this study since the goal is to obtain an in-depth understanding from the security professionals' perspectives.

In a quantitative approach, statistical testing is used to compare how the dependent variable is affected by the independent variable (Shahri, Ismail, & Mohanna, 2016). Statistical tests like *t*-tests and analysis of variance are used in a quantitative method to perform objective comparisons (Swanson, 2017). Additionally, quantitative methods are best suited for large samples and testing of theories and assumptions using statistical analysis (Elaoud & Jarboui, 2017). The techniques used to analyze quantitative numerical data obtained from surveys, financial reports, and evaluations include descriptive statistics, predictive statistics, and Bayesian modeling (Gibson, 2016). Since this study does not involve comparisons, the collection of numerical data, or testing theories, a quantitative approach would not be appropriate for this study.

A mixed-methods approach is a combination of both qualitative and quantitative approaches or data collected in one type of approach converted and analyzed using the other

approach (Gibson, 2016). Kalmakis, Chandler, Roberts, and Leung (2017) employed a mixed-method approach where explanatory descriptions from qualitative data, collected from online focus groups, were used to enhance the quantitative findings of data collected from online questionnaires. Barnett, Livingston, Perdue, Morgan, and Fogel (2017) conducted a mixed-methods study where quantitative and qualitative data were collected using Survey Monkey; IBM SPSS was used to determine the mean and standard deviation, and the frequency and percent to describe the continuous and categorical variables respectively for the quantitative data; while thematic analysis was used to identify, analyze, and report patterns of the qualitative data. Although this method includes a qualitative component, numerical and statistical data is not collected, therefore the mixed-methods design is not appropriate for this study.

Research Design

Four qualitative research designs--ethnography, phenomenology, narrative, and case study--were considered but only the multiple-case study research design will be used for this study. In an ethnographic study, the researcher is immersed in the participants' environment where the experiences of the participants may be observed within context allowing the researcher to accurately record and understand the participants' perspectives, behavior, and activities (Alftberg et al., 2018; Belak, Madarasova Geckova, van Dijk, & Reijneveld, 2018; Rosenfeld et al., 2018). Researchers may also collect empirical insights about social practices within working units and organizations that define a culture (Alyahya, Hijazi, Al Qudah, AlShyab, & AlKhalidi, 2018; Percy, Kostere, & Kostere, 2015). Since this study's focus is on exploring the security strategies used by IT security professionals and not the social interactions between the IT security professionals, ethnography is not a suitable research method for this study.

A phenomenological approach is geared towards exploring and obtaining an in-depth understanding of the experience being studied and not that of the individuals having the

experience (Kruth, 2015). Phenomenology commonly utilizes intensive, open-ended interviews to explore and understand a phenomenon from the participants' eyes (Harrison, Burress, Velasquez, & Schreiner, 2017). Gustafsson, Nyström, and Palmér (2017) defined a phenomenon as something that is perceived by human consciousness, such as a lived experience; thus, a phenomenological study focuses on the lived experience of participants within the context of interest (Sun et al., 2016). Although BYOD may be considered a phenomenon, the focus is on exploring the security strategies employed by IT security professionals and not the lived experiences of the participant in relation to BYOD; therefore, phenomenology is not a suitable method for this study either.

A narrative research method allows researchers to explore the participants' lived experiences through stories of past, present, future or hypothetical events (Clandinin, Cave, & Berendonk, 2017; Kostov, Rees, Gormley, & Monrouxe, 2018). McKail, Hodge, Daiches, and Misca (2017) conducted a qualitative narrative study where the participants were asked, in an audio-recorded interview, to tell their life stories in their own voice and language without interruptions. The narrative method will not be used since the participants' life story is not part of the study.

A case study research method is a flexible but challenging social science research methodology that asks the *how* or *why* a phenomenon works (Cope, 2015). Researchers use a case study approach to explore, explain, or describe a real-world phenomenon within the context of the study (Durodola, Fusch, & Tippins, 2017). In a case study design, data may be collected from interviews, observations, documents, and artifacts to provide an in-depth understanding of a case where a case may be a specific individual, event, or series of events (Kruth, 2015). A multiple-case study allows the researcher to explore and contrast the data between cases resulting in a more robust and complete analysis (Jackman, Crust, & Swann, 2017). The analysis performed in

a multiple-case study may be *within-case* where a detailed description of each case and its themes are presented or *cross-case* where the themes across the cases are compared (Houghton, Murphy, Shaw, & Casey, 2015). This study seeks to explore and describe IT security strategies used to secure networks where BYOD is permitted across multiple university campuses, making the multiple-case study approach the most appropriate research method to use for his study.

In qualitative research, achieving data saturation is necessary to assure that all information regarding the topic of interest has been collected where no new information or themes are discovered (Bishop & Cregan, 2015; MacLure & Stewart, 2018). To increase the chances of reaching data saturation, participants with experience of relevance are selected using the purposive sampling method (Moore, Blom, Whitehouse, & Gooberman-Hill, 2017; van Rijnsoever, 2017). The researcher continues to recruit participants and collect data until data saturation has been reached (Meintjes & Nolte, 2015; Perry, Johnson, Popat, Morgan, & Gill, 2018). To ensure data saturation employed the purposive sampling method and continued to interview qualified participants until no new themes emerged from the data.

Population and Sampling

For this study, I used the purposive sampling method. Purposive sampling was used to select participants that met a specific set of predetermined criteria for a research study (Durosaiye, Hadjri, Liyanage, & Bennett, 2018). Being the recruiting method of choice for case studies, purposive sampling provided an in-depth understanding from the participants' perspective (Dahl, Larivière, & Corbière, 2017). As a non-probability sampling method, researchers may deliberately select knowledgeable individuals to participate and not be bound to any specific number of participants (Eshtaiwi, Badi, Abdulshahed, & Erkan, 2018). Homogenous sampling is a type of purposive sampling method where participants with characteristics and traits appropriate and applicable to the study are selected (Oguz Hacat, 2018; Roache & Kelly, 2018).

When using purposive sampling, the sample size is determined when data saturation has been reached (Mammen, Hills, & Lam, 2018). Additionally, Manera, Craig, Johnson, and Tong, (2018) stated that saturation is reached when little or new information has been identified in further interview sessions. Using the purposive homogenous sampling method allowed me to select participants who are professionals in their field allowing for quality responses and information. More in-depth information regarding BYOD security strategies in a university network environment may be obtained using purposive sampling based on the following predetermined set of inclusion criteria: (a) working in a department on one of the 10 UC campuses, (b) experience managing a BYOD supported network environment for at least two years from a security perspective, and (c) the BYOD-enabled environment must have at least 50 users.

Fugard and Potts (2015) reported that the number of recommended participants for small projects involving interviews ranged from 6 to 10 participants while data saturation had been observed in interviews with as few as 6 participants and as high as 17 participants. I started by identifying and interviewing 8 participants who met the inclusion criteria and continued to interview addition participants until data saturation was reached. Holton, Joyner, and Mash, (2018) and Kooij, Groen, and van Harten, (2018) stated that data saturation is achieved when no new information has been identified after the interviews (Holton, Joyner, & Mash, 2018; Kooij, Groen, & van Harten, 2018). In total, I interviewed 10 participants where redundant information was observed after interviewing the 9th participant. While no new data was achieved after interviewing 9 participants, I decided to interview one more participant to ensure that I had truly reached saturation. Interviewing participants until no new insights were uncovered ensured data saturation (Tang, Zhou, Chan, & Liaw, 2018). Mammen et al. (2018) indicated that data saturation was determined by the data depth and how the sample size was established, not by the size of the sample.

Ethical Research

The ethical treatment of human subjects is an important factor in modern-day research. The premise of ethical research is built upon the Nuremberg Code of 1948--established as result of the horrific experimental research on human subjects by Nazi doctors and scientists during World War II; the 1964 Declaration of Helsinki--developed by the World Medical Association as a set of ethical principles or codes that researchers must adhere to when conducting studies involving human subjects; and the 1979 Belmont Report--issued by the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research as a framework for conducting research involving human participants outlining three core principles: respect for persons, beneficence, and justice (Artal & Rubenfeld, 2017; McKenna & Gray, 2018; Ross, Iguchi, & Panicker, 2018). The researcher has the moral and ethical responsibility of ensuring that no harm comes to the participants due to participating in the study.

The informed consent process in research assures that the participants are fully informed about the nature of the research, comprehend the risks and benefits involved, are competent and lucid to make decisions, and participate voluntarily without coercion (Kadam, 2017; Sil & Das, 2017). Participants will be presented with a consent form to sign that includes the background information of the study, the procedures that the participant will be asked to follow, assurance that participation is completely voluntary, identification of risk and benefits, compensation information, privacy declarations, and contact information to establish trust between the researcher and the participants. Urban and Schweda (2018) noted that even after obtaining written informed consent, participants were still free to withdraw from the study at any point in time without the need for reason nor explanation. The participants in this study may also withdraw from the study by contacting the researcher by phone or e-mail and simply state their desire to be removed from the study.

The use of incentives as a recruitment strategy varies from study to study. Largent and Lynch (2017) pointed out that money may be used for reimbursement of research-related expenses, compensation for time and inconvenience, an incentive to overcome lack of interest, and token of appreciation; however, care must be taken to not introduce coercion, create undue influence, or offer undue inducement. Li et al. (2018) presented participants with an incentive gift valued at $12 after completing the focus group while Ha and Pepin (2018) offered no incentives or reimbursements to participants. Though there will be no incentives or reimbursements offered in this study, participants will receive a $5 Starbucks gift card at the end of the study in appreciation for their participation. To ensure that participation was not driven or influenced by the outlook or anticipation of a gift or reward, participants were not informed that they would receive a gift nor would they know the type and value of the gift until after the study had completed.

Researchers all over the world have the responsibility to protect research participant data. Origlia Ikhilor et al. (2018), in accordance with the international and ethical guidelines referred to as Good Clinical Practice, de-identified and secured participant data for ten years at a secure facility. The identity of the participants in this study will be held confidential by using participant number in place of the participants' names where the real identity of the participant is known only to me. All records will be securely stored for 5 years after the completion of the study in a lock-box then shredded or deleted accordingly. The Walden IRB approval number for this research study is 03-18-19-0659129.

Data Collection

Instruments

I was the primary data collection instrument for this study by meeting with the participants to conduct in-depth semistructured interviews and retrieving publicly-accessible

documents from the organizations' publicly facing websites. In qualitative research, the researcher or principal investigator are often the primary data collection instrument (Houghton, Casey, & Smyth, 2017; Murdoch-Flowers et al., 2017; Siew, Mazzucchelli, Rooney, & Girdler, 2017).

I conducted semistructured interviews and ask open-ended questions to probe and elicit in-depth responses from the participants. Broom, Broom, Kirby, Gibson, and Post (2017) used semistructured interviews to draw out the experiences of the participants. Semi-structured interviews are also used to obtain detailed knowledge, attitudes, and perceptions (Colder Carras et al., 2018; McLean et al., 2017). Semi-structured interviews allow the researcher to probe for motivations and experiences from participants (Jackson, Snyder, Crooks, & Lavergne, 2018). While having a structured framework, semistructured interviews allow for flexible and fluid dialog between the researcher and the participants (Xerri, 2018).

To keep my semistructured interviews on track, I used an interview protocol (see Appendix C). According to Kallio, Pietilä, Johnson, and Kangasniemi (2016), the credibility, confirmability, and dependability of a study using semistructured interviews stem from a well-developed interview guide. A semistructured interview guide provides structure to the interview and may include both open- and closed-ended questions to assess participants' experiences, perceptions and attitudes (Ippolito et al., 2017; Wendot et al., 2018). An interview guide helps maintain focus and ensures consistency across all participants (Schröder, Soliman, & Riebisch, 2018). Schröder et al. (2018) developed an interview guide that contained three parts: 1) establishing the participants' background and experiences, 2) identifying areas of concern, and 3) discussing the activities the participants perform to address the area of concerns. Using an interview protocol (guide) ensured that the interviews stayed on track and consistent from one participant to another. I started the session by introducing the study and reminding that

participation was entirely voluntary and that the participant may withdraw at any time without needing a reason. Before starting the recording, I checked with the participant for any objections and if there were, I would end the session and thank the participant; and if not, I proceeded with the interview and asked the questions. After all the questions were asked and answered, I concluded the interview by reminding the participant of their rights to withdraw and provided them with instructions on how to do so.

I collected policy and procedural data from each campus' website to strengthen the credibility of the study. In addition to semistructured interviews, publicly-accessible documents may also be collected to provide additional insight like policies and business strategies obtained from the organizations' websites (Campbell, Manns, Soril, & Clement, 2017; Nilsen & Størkersen, 2018). Cunningham, Menter, and Young, (2017) posits that having more than one data source increases the robustness of a study and identified primary data collection methods as interviews, focus groups, observations, and onsite workshops and participative events; and secondary data collection methods as data, literature reviews, web-based data and reports, and documentation. The policy and procedural data from each campus' website will be used as a second data source and strengthen the credibility of the study by data triangulation.

To enhance the reliability and validity of the data collected from the semistructured interviews, I scheduled face-to-face follow-up interviews with the participants to check and validate my summary and interpretations for accuracy using member checking. Trustworthiness and quality of qualitative data may be enhanced by employing member checking where researchers may confirm their understanding of the interview responses with the participants (McGrath, Palmgren, & Liljedahl, 2018). The data may be considered credible and the research valid if the participants confirm that the data collected are accurate while also controlling and correcting potential researcher bias (Smith & McGannon, 2018). Thomas (2017) stipulates that

aside from not being very useful in theory development, posing an inconvenience to participants, and resulting in insignificant changes, member checking is appropriate when the purpose is to ensure an accurate representation of participants' perspectives or experiences where case studies are used. To promote and ensure that the participants are willing to participate in member checking, I asked the participants during the consent procedure.

Data Collection Technique

My primary source of data came from semistructured interviews conducted with the aid of an interview protocol (see Appendix C). The interview protocol provided a scripted roadmap to help keep the interview consistent and on track. While providing consistency, an interview protocol permits participants to elaborate beyond the original questions and interviewers to insert follow-up questions (Fox, Bacile, Nakhata, & Weible, 2018). An interview protocol contains close- and open-ended questions aligned with the research question allowing for flexibility and increased flow (Haude, McCarthy Veach, LeRoy, & Zierhut, 2017; Johnson & Menna, 2017). The interview protocol (see Appendix C) used is broken down into three main sections: preinterview, interview, and postinterview.

Before asking the interview questions, preinterview tasks were completed. Because of security protocols and room availability, I was not able to gain access to the meeting room to set up and test the recording equipment prior to the scheduled interview time at the predetermined location and had to test the equipment before the interview session. The researcher must disclose the nature of the study to the participant and give the participant the choice to participate or not and obtain informed consent (McKenna, Myers, & Newman, 2017). I provided an overview of the study, explain the interview process and informed the participants that the sessions were to be recorded and at the follow-up interview, they would have the opportunity to check and confirm my interpretation of the information obtained during the interviews. Before the interview can

proceed, informed consent is required, and the participants must understand that participation is voluntary (Warburton, Moore, & Oppenheimer, 2017). Winters, Carvalho, and Oliver (2017) provided information to participants regarding informed consent and anonymity assurance procedures to help ease participation concerns. After receiving informed consent, I reminded the participant that they can withdraw at any time and the data collected will be destroyed to preserve their privacy and that de-identification will be used to maintain anonymity.

I conducted semistructured interviews face-to-face at a quiet location of the participants' choosing. To avoid mobility and accessibility issues, Pretto (2017) permitted the participants to select the interview locations. Kang and Jeong (2018) selected a place where the participants would feel comfortable, like in their homes, a public place or a meeting room. While interviewing over the telephone is an option, the telephone does not allow as much access to the participant nor present an ideal setting to build rapport and promote deeper discussions (Farooq & de Villiers, 2017; Ronchi, Lewis, Hauck, & Doherty, 2018). Semi-structured interviews are flexible by allowing the researcher to go off script and the participants to ask questions promoting dialogue while accommodating the differences from one interview to another (Farai & Mugove, 2017). Farai and Mugove (2017) added that aside from the benefits, semistructured interviews also have weaknesses like asking leading questions, repeating questions that had already been addressed, the researcher failing to listen closely to the responses, and the questions may be too vague (Farai & Mugove, 2017). The locations of the interviews were left to the participants' discretion with the requirements that the selected locations must be free from interruptions and distractions to ensure that the participants were comfortable and relaxed.

There are two types of interview questions, closed-ended and open-ended questions. Closed-ended questions are used to establish or confirm the participants' background like professional identity and training; whereas, open-ended questions are used to clarify the

participants' story and allow for more spontaneous responses (Jaskiewicz, Combs, & Rau, 2015; Myers et al., 2018). Semi-structured interview using both open- and closed-ended questions, provides a balance between being systematic and keeping a conversational tone while allowing for open dialog and follow-up questions (Jenness & Calavita, 2017). To confirm details regarding the participants' qualifications, I started with closed-ended questions then progressed to open-ended questions to encourage the open sharing of information pertaining to the study topic (see Appendix C). Unclear responses were met with follow-up questions to clarify areas of ambiguity. During the responses, I took notes and observe the participants' demeanor.

After all questions were asked and the participants had no more information to add, I concluded the interviews. I thanked the participants for their time and remind them how the data will be kept confidential, how they may contact me to withdraw if they change their minds, and that we would meet again to discuss and check my summary and interpretations for accuracy. Member checking is a technique used to confirm the agreement between the researcher's interpretation and the participants' perspectives (Raymond, Profetto-McGrath, Myrick, & Strean, 2018). Cai, Kunaviktikul, Klunklin, Sripusanapan, and Avant (2017), during data analysis, used member checking to ensure that the data was reliable. During the member checking process, the participants were asked to make changes to the summary so that the information collected accurately conveys what they intended to say (Harding et al., 2018). I used member checking to ensure the validity and reliability of the collected data.

In addition to collecting data through semistructured interviews, I also reviewed publicly-accessible information from the participants' organization websites. The use of additional data sources helps provide clarity and validity to the study through triangulation where the data collected from different sources are corroborated (Cardoni, Dumay, Palmaccio, & Celenza, 2018). Publicly-accessible sources that may be used for triangulation and establishing context

validity include company websites, newspaper articles, journals, reports, and statistics (Sarkar, Osiyevskyy, & Clegg, 2018). Fox, Gardner, and Osborne (2018) obtained governance documents from publicly-accessible websites using key search words to collect information in addition to surveys and semistructured interviews. A downside to searching for publicly-accessible documents on the Internet is that accurate or useful information may not be available (Ellwanger et al., 2018). I searched the organizations' websites for policy documents and information to supplement and support the data collected from the semistructured interviews.

Data Organization Techniques

Different types of data are collected like logs, interviews, and archival documents. Having a method for organizing them will allow for efficient access and use of the data during analysis. Ranney et al. (2015) presents organizing qualitative data as one of the steps necessary for establishing validity and reliability in an interview-based qualitative study. Field notes during interviews improve the accuracy of data interpretation (Gorniewicz et al., 2017) and are kept in journals along with postinterview reflections (Clayton, Medina, & Wiseman, 2017). While collecting data, protecting the participant's privacy is highly important. Any identifiable information must be removed and anonymized and replaced with pseudonyms (Davidson et al., 2014; Grossoehme, 2014). The journal will contain the dates and times of the entries, but the names and locations of the participants and organization will be obscured to protect the identity of the participants.

The interview recordings were transcribed prior to analysis. The validity of interviews is increased through recording and transcription of the sessions (Madar, Adini, Greenberg, Waisman, & Goldberg, 2018). McGrath et al. (2018) identified that verbatim transcription is a common form of transcription that includes pauses, giggles, and other verbal queues that many researchers elect to perform to get more acquainted with the data. According to Scheel-Sailer,

Post, Michel, Weidmann-Hügle, and Baumann Hölzle (2017), the first step after transcribing and anonymizing the interviews is to descriptively summarizes the interview and tag passages related to the study topic. I transcribed the audio recording verbatim using Microsoft Word and de-identified the participants and organizations involved to further preserve confidentiality and privacy. All printed and electronic raw data will be secured in a locked container for five years then shredded.

To analyze the collected data, Ruthven (2017) entered and organized field notes, interview transcripts, and collected media into a computer-assisted analysis software program. NVivo Qualitative Data Analysis is a software package used by some researchers to manage, query, model, code and identify themes in unstructured qualitative data, and formulate reports (Ruwhiu, Amoamo, Ruckstuhl, Kapa, & Eketone, 2018; Sepasgozar, Davis, Loosemore, & Bernold, 2017). I used NVivo 12 Plus to assist in coding and identifying themes from the interview transcripts and interviewer notes.

Data Analysis Technique

The data analysis technique I used for this multiple-case study was thematic analysis. By thoroughly examining the interview transcripts, themes may be identified inductively (Goldstone & Bantjes, 2017). According to Braun and Clarke (2006), thematic analysis is a recursive and not a linear process that should not be rushed; and provided a six-phase analysis process consisting of familiarizing with the data, generating initial codes, using the codes to identify themes, reviewing the themes, refining the themes, and producing the report. There is a chance that no common themes will emerge; however, a broad range of experience may be revealed (Lusk, Dobscha, Kopacz, Ritchie, & Ono, 2018). I familiarized myself with the transcripts, code, and searched for emerging themes with the aid of NVivo 12 Plus.

To increase validity, enhance credibility, and mitigate bias in this study, I used data triangulation. Triangulation is a strategy used in qualitative research to validate a study by utilizing data from multiple and different sources (Davis et al., 2018). There are four common types of triangulation: theory triangulation--employing multiple theories or hypotheses to examine a phenomenon; data triangulation--use of multiple data sources; methods triangulation--involving multiple methods or data collection techniques; and discipline triangulation also referred to as investigator or researcher triangulation--involving multiple observers, respondents, or coders (Abate & Krishnaiah, 2017; Lewis, 2017; Tenório, Loos, & Tenório, 2017). Huijnen, Lexis, Jansens, and de Witte (2017) used data triangulation to ensure integrity and validity.

Interview transcripts, notes, and publicly-accessible documents must be prepared before importing into NVivo 12 Plus. The transcripts must be de-identified and formatted using header styles for easy processing by NVivo. Using NVivo, themes may then be extrapolated and categorized according to the conceptual framework to answer the research question (Denedo, Thomson, & Yonekura, 2018). The first phase of Braun and Clarke's (2006) thematic analysis process is familiarization with the data. I listened to the audio recordings and personally transcribed the interviews prior to loading the transcripts into NVivo to generate the initial codes. NVivo has a "node" feature that may be used for generating initial codes (Vosper & Hignett, 2018). Phase three, four, and five are iterative steps and were performed in NVivo. Word clouds can be created in NVivo to view the frequency of words and identify themes (Shah, Husnain, & Zubairshah, 2018). Once the themes were finalized, the analysis completed with a report of the findings.

The collected data was analyzed to identify key themes that were correlated with concepts from PMT and security practices relating to BYOD. Hamilton et al. (2018) compared the emergent themes to existing guiding principles, frameworks, models and recommendations

after identifying the themes. The motivation to engage in protective behavior is a result of the perception of threat and the belief that the threat can be neutralized (Sanderson et al., 2017). The emergent themes aided in understanding the motivation factors leading the IT security professionals to take on a protective role and the strategies employed to support and secure a network open to BYOD.

Reliability and Validity

To ensure quality, strategies for establishing reliability and validity are integrated into the study design. Reliability and validity are crucial when the findings in a qualitative study are to be generalized and applied to a larger population (Ennis, Ablett, Taylor, & Lal, 2018). The reliability and validity of findings and improvement in triangulation may be improved by using various methods for collecting qualitative data (VanLeeuwen & Torondel, 2018). Guba and Lincoln (1994) presented the four criteria of trustworthiness in qualitative studies: dependability, credibility, transferability, and confirmability.

Dependability

I employed data triangulation to increase dependability. Dependability is repeating the study procedure under the same conditions and obtaining the same results (Bongiovanni, Leo, Ritrovato, Santoro, & Derrico, 2017). Brook, Salmon, and Knight (2017) triangulated using data from focus groups, interviews and questionnaires to establish data credibility and dependability. I triangulated by cross-referencing semistructured interview data from multiple case studies and publicly available documents. Consistent coding and achieving data saturation helps to increase the dependability of repeating the outcome (Flax et al., 2017).

Consistency in coding was achieved using NVivo Plus. NVivo Plus capabilities include importing and analyzing textual data, creating codes, querying text, recording memos, exporting codebooks with definitions and hierarchies; allowing users to analyze audio, video, datasets,

social media comments, and Microsoft Outlook e-mail exports; creating concept maps, predefined and customized reports, and visuals of social media output relationships; and automatically analyzing data to identify themes and sentiments (Phillips & Lu, 2018). Mercer-Mapstone, Rifkin, Louis, and Moffat (2017) used NVivo Plus to code a portion of the dataset into subthemes. Panagiotis (2017) used NVivo Plus to auto code the interview responses and generate a word cloud and treemap to illustrate the frequencies of the words from the interviews. The data collection process was iterative; hence, I conducted interviews according to the interview protocol until saturation where no new information emerged. I recorded observations and rich descriptions of the context and settings in a journal for each location. Saturation was reached when no new information was attained after member checking where additional probing was performed.

Credibility

In this study, I enhanced and established credibility through member checking where I ask the participants to review the interview summary for accuracy; and using data triangulation by conducting multiple case studies and collecting data from in-depth semistructured interviews, and publicly available documents. Credibility is the truthfulness in the findings drawn from the interpretation of the participants' views and data (Korstjens & Moser, 2018). Winkel, Honart, Robinson, Jones, and Squires (2018) enhanced the credibility of their study using reflexive memos, interview notes, and member checking to mitigate subjectivity. Mazerolle, Myers, Walker, and Kirby (2018) also used member checking along with researcher triangulation and a peer-review process to establish credibility. To strengthen the credibility and reliability of their research findings, Cooper, Leon, Namadingo, Bobrow, and Farmer (2018) triangulated the data through in-depth interviews and focus groups. Data collected from the semistructured interviews were direct accounts from the participants' perspectives while the documents retrieved from

publicly-accessible sites were policy or governance-related. Triangulation using these different types of data ensured the credibility of this study.

Transferability

I ensured transferability by maintaining detailed notes throughout the study. By using purposive sampling, transferability was further enhanced. Transferability is the ability to relate the results of the study to other contexts using other participants (Korstjens & Moser, 2018). Dadzie, Aziato, and Aikins (2017) ensured the transferability of findings in a similar context by providing a detailed description of the research settings, methodology, and background of the participants in addition to using an interview guide and maintaining an audit trail. To increase transferability, I logged thick descriptions of the context in a journal in addition to the participants' responses. Having thick descriptions would allow other researchers to decide whether the findings may be transferred. Martin et al. (2018) and Blanchard et al. (2018) employed purposive sampling to test the transferability of constructs in different contexts. The participants were recruited using a purposive sampling method where IT security professionals meeting a set of desired characteristics or criteria were selected. Transferability may be attained by selecting participants using the same criteria.

Confirmability

To ensure confirmability in this study, data triangulation was used along with maintaining a reflective and reflexive journal to establish an audit trail. To achieve confirmability, Jansen van Rensburg, Maree, and Casteleijn (2017) used data triangulation and an audit trail. Luctkar-Flude, Tyerman, and Groll (2018) increased dependability and confirmability by maintaining a detailed audit trail throughout the data collection and analysis process. Henningsen, Sort, Møller, and Herling (2018) ensured confirmability using reflectivity to document understanding before data collection, memos, decision records, and research logs; thus,

creating an audit trail throughout the study. I triangulated using documents and interview data from different organizations at different campuses. Even though the campuses are part of one system, each operates autonomously from the other.

Transition and Summary

Section 2 reintroduced the purpose of the study which is to explore the strategies IT security professionals working in a university setting use to secure an environment to support BYOD in a university system and rich descriptions of the researcher's role in the study, participant selection criteria, the research method and design, the sampling strategy, the data collection and analysis process, and the strategies for establishing trustworthiness. I am the primary data collection instrument and will be conducting semistructured interviews with the aid of an interview protocol and collecting additional data from publicly-accessible websites. The participants will be purposively sampled according to a set of defined criteria. Data triangulation, member checking, audit trails and detailed journal notes will be used to increase rigor and trustworthiness of the findings. Section 3 will include the presentation of findings, application to professional practice, implications for social change, recommendations for action and further research, and conclusion.

Section 3: Application to Professional Practice and Implications for Change

Overview of Study

The purpose of this qualitative descriptive multiple-case study was to explore the strategies IT security professionals working in a university setting use to secure an environment to support BYOD in a university system. I obtained data for this study through semistructured interviews with 10 IT security professionals from six campuses of the UC system. All of the IT security professionals were current UC employees who had worked at least two years at their respective campuses; each supported a network with at least 50 users that permitted BYOD or personally owned mobile devices to connect to the network. After each of the interviews, I conducted additional member-checking interviews where summaries of the initial interviews were presented to each of the IT security professionals for review and confirmation of accuracy; doing so gave the participants the opportunity to offer their corrections if I had made an error in my interpretation of the information collected. Ten semistructured interviews were conducted, but saturation was achieved where no new data were collected after the ninth interview. I retrieved publicly-accessible documents and information comprised of IT security policy documents, meeting notes, planning documents, and IT security support web pages from the campus outward-facing websites for each participant with the help of the Google search engine. The publicly-accessible documents were used in conjunction with researcher notes for triangulation and validation of the findings.

Presentation of the Findings

The overarching research question of this study was, What strategies do IT security professionals working in a university setting use to secure an environment to support BYOD in a university system? In this section, I discuss the five major themes that emerged from data triangulation of multiple case studies where the data were obtained from semistructured

interviews and publicly-accessible documents. I interviewed 10 participants from six UC campuses, in addition to performing an Internet search using the Google search engine that produced 50 usable references. The publicly-accessible information consisted of support pages, planning documents, meeting notes, and local security policies from six campuses and the Electronic Information Security Policy (IS-3) from the University of California Office of the President. Transcripts of the initial interviews and follow-up member checking interviews, along with the publicly-accessible documents, were imported into the NVivo software. Using NVivo, I organized and coded the data to identify four major themes that aligned with PMT (Rogers, 1975), the framework used in this study: (a) the ubiquity of BYOD in higher education, (b) the strategies used to connect mobile devices to the campus network, (c) the effectiveness of strategies to mitigate BYOD risks, and (d) the IT security professionals' task include identifying and implementing network security strategies.

Theme 1: BYOD is Ubiquitous in Higher Education

The first major theme identified was that BYOD is ubiquitous. Students, staff, and faculty are bringing and connecting their personal mobile devices to the university network for educational and business use. In a recent study, Raghunath, Anker, and Nortcliffe (2018), stated that for every student, at least two devices like smartphones and tablets are brought on campus while staff and faculty are using mobile devices to enhance the learning experience; these statistics support the theme of BYOD being ubiquitous. The concept and phenomenon of BYOD began in the corporate sector in 2009 (Cheng et al., 2016) and has now penetrated the academic sector into schools and universities (Stevenson & Hedberg, 2017). Before an IT security professional can secure and protect a network where BYOD is present, knowledge of the environment is imperative (Aramă & Emandii, 2017). The various type of personal devices brought on campus by staff, faculty, and students contribute to the ubiquity of BYOD in higher

education. Table 1 lists the number of users and devices each participant reported supporting. The average number of devices to users is about 1.5 to 1.

Table 1

Users and Endpoints Supported

Participant	Users	Devices
1	12,500	35,000
2	4,500-5,000	15,000-20,000
3	67,000	-
4	20,000	-
5	-	1,000
6	8,000	12,000-16,000
7	18,000	36,000
8	26,000	-
9	60,000-70,000	50,000-60,000
10	300	-

Classifying BYOD devices. Personal devices are owned and brought in by faculty, staff, and students and connected to the campus networks to do administrative-, research-, and education-related work in addition to engaging in other online activities. Although all 10 participants agreed that BYOD included everything and anything that could connect to the network, I shortened the list of BYOD devices for the study to smartphones, tablets, and laptops. Three of the 10 participants included IoT-type devices such as temperature sensors, microscopes, storage devices, game consoles, televisions, sprinklers, and doorbells in addition to the aforementioned devices. Hence, any network-enabled portable devices brought on campus regardless of who purchased it was considered BYOD (see Table 2). Eight participants responded that there were no restrictions as to which devices could connect to the network, therefore enabling the proliferation and use of BYOD.

Table 2

Participants' Perceptions of BYOD Devices

Participant	Devices perceived as BYOD
1	IoT devices--temperature sensors, Xboxes, Smart TVs, cell phones, computers, Amazon Alexa, Q NAS, and toasters.
2	Anything--cell phones, iPads, routers, and access points.
3	Anything and everything--laptops, Chromebooks, smartphones, desktop computers, sprinkler systems, and IoT.
4	Phone, laptop, computer, tablet, mobile devices, or anything that can connect to the wireless network.
5	Anything that can connect to the network.
6	Phones, tablets, laptops, and doorbells.
7	Everything--cell phones, tablets, laptops, or anything that can connect to the wireless network.
8	Every endpoint, gaming devices, wireless devices, anything that can connect to the wireless using WPA2.
9	Pretty much anything--IoT, cell phones, Xboxes, and Philip Hue devices.
10	iPhones, iPads, computers, smartphones, and tablets.

The participants' responses are substantiated by information collected from two policy documents (including IS-3), one training document, and three IT support pages. IS-3 lists "[a]ll devices, independent of their location or ownership, when connected to a UC network or cloud service used to store or process Institutional Information" (University of California, 2019, p 1) as being within the scope of the security framework, thus indicating that BYOD devices are permitted on campus. All seven of the documents referenced some form of a portable computing device like laptops, smartphones, and tablets while four documents add network-capable devices to the list, hence supporting the inclusion of IoT as part of BYOD (see Table 3).

Table 3

References to Mobile Computing Devices Versus Other Network-Capable Devices

Data source	Computing devices (BYOD)	Other (IoT)
Participants	10	3
Documents	7	4

Factors supporting the practice of BYOD. How and when BYOD first appeared on the campuses overall is unclear, but its ubiquitous presence on university campuses is certain. According to Participant 3, the BYOD phenomenon has been around ever since the Internet was available; however, eight participants suggested that BYOD on campus, in relation to staff and faculty, may be motivated by financial or flexibility factors. Two documents included discussion of the impending arrival of BYOD and the observation that not every department was prepared or ready to support the phenomenon while the other two documents had as their focus the preparation and use of BYOD. Financially, some campuses may not possess the funds or have room in their budget to provision computing equipment to their staff and faculty. Participant 10 commented, "if [campus] had to pay for all those devices that allow people to remain connected, it would quickly be out of control." In a recent study, cost savings were identified as one of the benefits of BYOD by Kadimo et al. (2018). According to Participant 8, personally owned devices are already being brought in and used by some faculty; Participant 1 confirmed this by adding that he provides support for the personal devices that are brought in by staff and faculty. One campus-support site stated, "[i]f you can bring it in, we'll work on it!," while adding that services included installing and configuring applications on BYOD devices. Table 4 lists the factors permitting BYOD to be used on the university campus and the number of participants and

documents implicating those factors. With faculty and staff buying and using their own devices, the campus is spared the cost of purchasing and maintaining the equipment.

Table 4

Factors Permitting BYOD

Factors	Participants	Documents
Financial	5	1
Flexibility	6	2
Open network	4	4

Regarding flexibility, Participant 5 noted the work-from-home situation where staff or faculty may have a university-issued desktop at work but do not want to constantly transport the device back and forth between locations. The use of a personally owned device allowed increased work flexibility. As for students, Participant 7 pointed out that students are mobile in this digital age of computing and suggested that the learning landscape is changing by going online to be more accessible to students. Students can use their personal devices anytime and anywhere to do homework, perform research, and submit assignments. Theobald and Ramsbotham (2019) acknowledged that the advancement in technology continues to influence the pedagogical approach to learning and BYOD provided a flexible means for students to connect and share information. Participants 4 and 5 included that BYOD allowed students the flexibility to choose the device that met their requirements and do what they need to do, thereby adding to the increasing use of personal devices in higher education. Furthermore, due to budgetary constraints, there may not be enough computing resources to allow every student access to a computer. Safar (2018) found that the overall academic performance of students using their own devices improved.

The academic environment was also a factor in allowing the use of BYOD on campus. Eight out of nine of the participants acknowledged that they were working in an academic environment and to allow and enable the freedom to learn, the security practice is to have an open network. Participant 8 stated that restrictions on how the campus community uses the computing resources were low to allow unobstructed freedom to conduct research and learn. Participant 1 and 3 acknowledged that the campus network environments have always been an open network to allow staff, faculty, and students to do whatever they needed for research and technical support was provided as needed. The concept of an open network in a higher education environment is supported by Singh et al. (2018) where 88.5% and 98.4% of the students had possession of personal computers and smartphones respectively. While publicly retrieved documents do not explicitly use the term "open network", one of the goals of IS-3 is to preserve academic freedom and research collaboration. The open network environment along with the financial and flexibility benefits are conditions supporting the widespread presence and practice of BYOD on university campuses.

PMT - Source of information. In this study, the PMT (Rogers, 1975) served as the conceptual framework used to examine the components that result in executing protective behavior. Current PMT studies look at protective actions performed to protect one's self. I sought to understand what motivates an IT security professional to protect a network environment where BYOD is permitted. The first component of the PMT is acquiring information about a certain condition or phenomenon, in this case BYOD being ubiquitous. The information may be drawn from observations of the environment or interpersonally through experience. Theme 1 provided the rudimentary understanding of the IT security professionals' knowledge of the number of devices in relation to the number of users, the different types of BYOD devices, the factors promoting the use of BYOD, and the network environment. In recent literature, Li et al. (2019)

stipulated that the more information a person has, the more willing the person would be to engage in cybersecurity measures. Martens, De Wolf, and De Marez (2019) identified the processing of sources of information as one of three consecutive processes of PMT with the cognitive mediating process and the intention to implement certain protection methods being the other two.

Theme 2: Accessibility Strategies for Mobile Devices

Accessibility includes the type of device connecting to the network, the type of data or information being accessed, and the number of endpoints on the network. While recognizing that BYOD is ubiquitous on campus, all 10 participants agreed that these personal devices are permitted to connect to the campus network and access the Internet as well as access campus data from anywhere Internet access is available.

According to Participant 9, personal devices are restricted from directly connecting to the hard-wired network however, access through the campus-wide wireless network may be established with valid credentials. When connected to the wireless network, users only have access to the public web space; while Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), and human resources (HR) information are completely segmented off. Inversely, Participant 5 claimed that anyone can connect their personal device into the network and be able to access "all of the information that you'd be able to access with [a] university-owned device." While Participant 7 echoed Participant 5's sentiments of being able to access everything on the campus network, Participant 5 specified that a user with a device connected to the network can access the printers, in addition to the Internet, if they have a valid active directory (AD) account. Two documents provided clarification, stating that security groups are used to administer access to resources like printers, scanners, and network drives and that devices connected to a physical network port need to be

requested so that the network switch ports may be configured to allow access under unique situations.

An advantage of BYOD is the ability to access information from anywhere a network connection can be established. Participants 4, 6, 9, and 10 mentioned that a user working from a remote location may access campus computing resources through a VPN connection. Using a VPN increases the security level of the Internet connection by establishing an encrypted tunnel between locations (Chen & Li, 2018). Two participants reported that students, faculty, and staff can download, install, and use the VPN service if valid credentials are used and information retrieved from the support sites of all six campuses confirmed that anyone with a valid computing account can access campus resources from outside the network through a VPN connection.

Even though VPN service, network segmentation, and access control measures are available, each campus is afforded some latitude by the University of California Office of the President to manage their networks as they see fit. The network managed by Participant 1 has a publicly-accessible IP address range with no outbound restrictions and does not require a login. Anyone that connects to the network would have full access to any publicly-accessible network resource. The IS-3 policy document explicitly indicates that in addition to providing a framework for consistency, it also supports local flexibility. Participants 4 and 9 acknowledged that exposure of sensitive data is a risk with legal repercussions, damage to reputation, and loss of productivity but is mitigated by the security access controls that are in place; however, the access controls pertain more so to university-issued devices which are encrypted and insured and not personally owned BYOD devices. A mobile security document listed phishing, malware, social media integration and permissions, GPS locators, near field communication (NFC) or Bluetooth, third-party applications, and public hotspots as some risks and threats to consider when using mobile devices like smartphones and tablets. If a personal mobile device is used, it must meet the campus

security requirements and be encrypted according to two other campus web pages discussing mobile devices and restricted data.

PMT - Threat appraisal. The second component of the PMT is assessing the threats. By considering the known and unknown threats, stakeholders are better prepared to defend against a cyber-attack (Happa, Glencross, & Steed, 2019). Having the necessary knowledge about associated vulnerabilities will help the organization mitigate potential risks (Limba, Plėta, Agafonov, & Damkus, 2017). The second theme covered the type and number of devices that were connecting to the network along with the type of data available on the network. In this study, the participants acknowledged that users can attach their devices to any network outside the domain network, establish a VPN connection, and be able to access information as if they were on a wired connection. Various systems and servers containing sensitive information are at risk of being compromised when an infected device connects to the network or when unprotected personal devices access malware-infected content. The threat assessment obtained from the second theme indicates that the security and access tools that are in place may not be enough to fully defend against the potential threats introduced through the use of BYOD.

Theme 3: The Effectiveness of Current BYOD Strategies That Minimize Risk

In addition to realizing that BYOD is ubiquitous, the level and degree of access a user may acquire, and the potential risks associated with BYOD, the strategies that are in place contribute to the IT professionals' demeanor towards personal mobile devices. In determining the effectiveness of network security strategies, nine out of 10 participants referenced auditing or reviewing metrics obtained from a combination of alerts, log files, and ticketing system. Miranda (2018) recommended that metrics be compiled to identify trends and determine the effectiveness of implemented strategies. Out of the nine participants who responded, three had indicated using at least two of the sources listed in Table 5. Three participants pointed out that setting an initial

baseline at the time of implementation then comparing the difference in the reported security incidents at a later point in time would provide the data needed to evaluate the effectiveness of a strategy; a decrease would indicate that the strategy had a positive effect.

Table 5

Metrics Used to Determine the Effectiveness of Strategies

Metric source	Participants (*f*)
Alerts	5
Log files	4
Ticketing system	3

The IT security professionals in this study expressed mixed feelings regarding their comfort level with the effectiveness of the current BYOD strategy. Three reported feeling comfortable; three, neutral; and four, uncomfortable. While not happy with the current security practice, Participant 1 felt that a balance between education and security helps to provide an environment that supports and encourages learning, some concessions were necessary and that a certain level of penetration was expected. When a device gets compromised or infected, it would be sent to the help desk to be wiped and re-imaged, if it was not connected to any internal systems. Participants 2 and 6 shared the sentiment, adding that they were doing the best as they could with the tools available to them. Despite the level of comfort being somewhat evenly spread out among the 10 participants, they all agreed that there was room for improvement.

The IT security professionals expressed their concerns regarding the current BYOD strategy which were placed into four categories: control, threats, environment, users, and organization (see Table 6). Most of the concerns were not having control over securing the BYOD devices and the data accessed, saved, and transmitted during their use; and the increase in the number of vulnerable or compromised devices and threats. Half of the IT security

professionals expressed concern over having open networks; however, the openness was by design to encourage and foster academic research and learning. The first of six electronic information security goals outlined in the IS-3 is to "preserve an environment that encourages academic freedom." This goal is immediately followed by protecting the privacy of individuals without monitoring or observation. Hence, IT security professionals are limited to how much security restrictions they may impose on the campus network.

Table 6

Categorization of Issues

Issue category	Participants (*f*)	Details
Control	6	Not knowing where the data is at Data being stored on personal devices and storage media Not having complete control over the personal device Stolen devices not being reported Devices are not properly secured
Threats	6	Advanced Persistent Threat (APT) Obsolete devices no longer supported by the manufacturer Malware like ransomware and viruses A compromised device accessing restricted data
Environment	5	Open network No Network address translation (NAT)
Users	3	Faculty not understanding the importance of cybersecurity Students pushing security and privacy boundaries and limits
Resources	2	Lack of human and financial resources

As students, faculty, and staff bring more personal devices with them to university campuses, the campus security offices are offering more classes designed to educate the users on the potential risks and the appropriate actions to take to secure a device and report when a device has been lost or stolen. One training document presented the issue of storing personal identity

information (PII) and electronic protected health information (ePHI/HIPAA) on unencrypted devices and that campus security policies prohibits such practices. Additional risk data, as indicated in the IS-3, includes payment card data (PCI), controlled unclassified information (CUI), student records (FERPA) and research data. In terms of accessibility, if a network access port is "hot" or enabled and connected to a network, anyone can plug in and access the Internet. The same level of access is also available through the wireless network. Beckett (2018) stated that educating and training users about certain cyber threats can reduce the risk of a security incident occurring and may be more effective than digital controls. The IS-3 contains a line item requiring that users must complete any required training before access is granted and documentation from each of the six campuses central IT site contains information regarding mandatory annual cybersecurity training.

BYOD can connect to the campus network from anywhere and the current strategies appear to have some effectiveness in mitigating and reducing the risk of direct and indirect attacks from bad actors through personal mobile devices; however, based on the data collected for this study, even with security controls and policies in place, IT security professionals are not completely at ease with the security implementations and BYOD. Yasin, Czuchry, and Small (2018) suggested that before security strategies can be implemented, a complete assessment must first be conducted followed by a security gap assessment, securing investments and resources, and changing the organizational culture towards security. At least half of the participants have identified areas of concern with the lack of control of the personal devices, external threats from malware and bad actors, and the open campus network environment but less than a third mentioned non-conforming users and lack of resources needed to support security strategies.

PMT - Threat appraisal (cont.). The third theme assessed the effectiveness of current mitigating strategies. Security policies, training requirements, and access control tools are

in place to mitigate and reduce the risk of protected information being accessed and being compromised; however, the participants are not entirely comfortable with the current strategies. The participants in this study acknowledge that students, faculty, and staff could access the campus network from anywhere using their personal devices. Participant 1 stated that "we try to be as proactive as we can, but the reality is, many a times[sic] when we get alerts, the infections are already in and they've already pinging servers or had attempted to hack our DCs." The open network design, the lack of control over the BYOD devices, and threats from internal and external sources were identified by at least half of the participants as concerns. Menard, Warkentin, and Lowry (2018) presented that the severity and potential chance of being vulnerable and falling victim to a threat is evaluated during the threat appraisal process and that the probability of executing a defensive action is also affected.

Theme 4: Identifying and Implementing Network Security Strategies Is an IT Security Professional's Task

The fourth and final theme was that the IT security professionals charged with maintaining and securing the campus network where BYOD is allowed must be involved in the network security strategy acquisition and implementation process in some capacity. Nine out of the 10 participants acknowledged taking various roles in the acquisition and implementation of security tools and strategies (see Table 7). Participant 1 was the only participant who stated involvement from conception to implementation of the security strategies where he and his co-worker regularly review alternative solutions, develop a proof of concept, gather information, and then present the data to management for review and approval; and if approved, they would design and execute the implementation plan.

Table 7

Role in Strategy Selection

Role	Participants (*f*)
Research	4
Testing	3
Recommendations	3
Acquisition	3
Implementation	3

Two job descriptions list configuring, designing, developing, implementing, and maintaining tools, systems and procedures as some responsibilities of the IT security professionals. Wilson (2018) reported that the risk of exposure to cyber-attack may be managed through good security technology that was designed and implemented by IT systems and security professionals with expertise and skills in data protection.

The years of experience in IT security for the ten participants were between 5 and 35 years. The knowledge and information gained over the years were attributed to on the job exposure, involvement in network and IT security activities, and formal education and training. Participant 1 stated that "as long as you've got good analytical and logical skills, you can really figure things out but…if you don't have a fundamental understanding of how a network operates and functions, you're just going to be lost" and added that obtaining certifications like the CompTIA and Cisco certifications would be beneficial. Two job descriptions from two campuses list the minimum number of years of experience from 2 to 4 years however, the minimum requirements include experience analyzing and interpreting security and event logs, working with security tools like firewalls and security information and event monitoring (SIEM) solutions, having knowledge of encryption, and be able to recommend appropriate controls.

The IS-3 lists the goals of the campus information security policy as preserving academic freedom and research collaboration, protecting privacy, maintaining confidentiality, protecting

integrity, and ensuring availability while following a risk-based approach. The participants identified security as providing a safe environment where duties and tasks may be performed without interference, ensuring that sensitive is available only to those authorized to access them, protecting computing resources from attack, minimizing risk, and follow the CIA triad principles of information security. Srinivas, Das, and Kumar (2019) concluded that a security standard includes security tools, concept, policies, risk management, and training. The participants in this study were familiar with security tools and strategies like firewalls, VPN, network segmentation or segregation, monitoring, logging, cybersecurity training, and security policies while encryption, patching, and mobile device management (MDM) were mentioned by less than half of the participants (see Table 8). The publicly retrieved documentation referenced firewalls, training, security policies, anti-malware, and encryption at a higher frequency. The data suggest that firewalls are the primary security tool used while MDM solutions have only been considered by a small number of campuses. Participant 4 noted that MDM was starting to be deployed to the campus while Participant 7 had just recently deployed multi-factor authentication (MFA).

Table 8

Mitigating Strategies and Tools Referenced by Participants

Strategies/Tools	Participants (*f*)	Documents (*f*)
Firewall and network access control	9	14
VPN	9	6
Network segregation (including campus Wi-Fi)	9	4
Monitoring and logging	8	6
Education	7	10
Security policies and standards	6	15
Antivirus/anti-malware/anti-exploit	5	15
MFA	5	6
Encryption	4	10
Patching	4	8
MDM	3	1

While there are tools in place, some participants offered suggestions to improve the current security strategies like placing the entire campus network behind a NAT, implementing 802.1X registration over Ethernet, improving faculty understanding and cooperation towards information security, improving collaboration between campus IT security groups, implementing a mobile device management solution, involving IT security professionals in security strategy discussions, and more controls over remote devices. Kumar, Zarour, Alenezi, Agrawal, and Khan (2019) stated that to design durable secure software, practitioners must be involved; this sentiment may be extended to developing and implementing security strategies. Participant 8 confessed that from a security standpoint there are gaps that need to be addressed, and Participant 9 added that "when it comes to BYOD, I feel it's a bit lacking." By including IT security professionals in the tool procurement process, the IT security professionals will be more vested in the solution and have better opinions towards the network security tools and strategies implemented.

PMT - Coping appraisal. The third component of PMT is assessing one's own ability to cope or deal with a threat. The participants', according to position description documents, primary job responsibilities are to perform tasks designed to secure data, systems, and networks. Every participant has at least 5 years of experience in the IT field and acquired experience and knowledge through formal education or former employment (see Table 9). According to Abdulkareem, Augustijn, Mustafa, and Filatova (2018) and Dragojevic, Savage, Scott, and McGinnis (2018) the coping appraisal component consist of response or adaptation efficacy and self-efficacy where the effectiveness of and the ability to adapt or perform the protective action or behavior are assessed respectively. The participants did not indicate or express any doubt or weakness in their ability to perform security-centric tasks or utilize the tools available to them. Participant 1 professed that he and his co-worker had become experts in working with their

security tools and if the tools are powerful and efficient, they can minimize the risk to their environment; however, when asked about his comfort level towards the security strategies towards BYOD, his response was, “[it] terrifies the hell out of me.”

Table 9

Initial Source of IT Knowledge

Source	Participants
Formal education or classroom instruction	6
Informal or on the job training	4

PMT - Coping modes. The coping modes component in PMT is the result of threat appraisal and coping appraisal with two possible outcomes, adaptive and maladaptive coping (Wang, Liu-Lastres, Ritchie, & Mills, 2019). Looking at the threat appraisal component of PMT for this study, 4 of the participants were uncomfortable with the current BYOD security strategy while 3 participants expressed that they were comfortable with the remaining 3 were neutral. Additionally, the lack of control of the BYOD devices was a common concern among 6 of the participants and the current security strategies may not be strong enough. Participant 3 stated that there has not been a lot of focus on BYOD “because people are so used to the BYOD thing here [on campus].” Regarding the coping appraisal component, the participants were unanimously confident in their knowledge of security practices but were divided in their opinion of the effectiveness of the security strategy. The sources of information, the outcome of the cognitive mediating process, and the implementation of the protective response influence the type of coping mode used in response to a given threat (Clubb & Hinkle, 2015). Because the source of information, the threat condition, the coping assessment, and the components of a strategy may change over time, it is not possible to determine which mode the participants would take.

Alternatively, the driving force that brings the participants to work is the personal satisfaction of helping others and the interest in technology. Seven of the participants shared that they enjoy interacting with and helping users resolve issues, learning and solving problems, contributing to the organization's mission, and most of all love what they do. Since the task of securing and protecting the data is embedded in the participants' job descriptions, the resulting coping mode may have been superseded by the sense of ownership and duty. Menard et al. (2018) concluded that employees who perceive ownership are more inclined to perform secure behaviors regardless of the PMT's self-efficacy and response efficacy.

Applications to Professional Practice

The intent of this study was to explore the strategies used to secure a higher education network environment to support BYOD by IT security professionals working in a university setting. The participants discussed their understanding of BYOD and the security implications and strategies associated with allowing personal mobile devices to connect to resources on the campus network. Guided by the PMT, the data collected was thematically analyzed resulting in four themes: BYOD is ubiquitous in higher education, accessibility strategies for mobile devices, effectiveness of BYOD strategies that minimize risk, and identifying and implementing the network security strategies is an IT security professional's task. The participants in this study identified BYOD devices as anything capable of connecting to the network, whether through a direct connection or VPN tunnel from a wireless or external connection, and that one of the challenges was visibility into how the devices were configured. Chung (2019) posited that if employees were equipped with the right tools and training, they would be capable of defending against malware threats like ransomware.

In addition to firewalls, VPN, subnetting, security policies and security training, security hardening the personal mobile devices with encryption, patching, anti-malware, and MFA may

further mitigate potential threats associated with BYOD. Since the greatest threat to information security is the human, having a cybersecurity training requirement may help keep the users informed and knowledgeable on how to identify and mitigate security risks (Ma'ruf & Rochman, 2019; Wirth, 2018). Users who have completed the training may have more confidence to cope with and avoid potentially malicious e-mails and websites. Furthermore, the user may be more empowered and inclined to pass the knowledge on to others like friends and family.

The participants in this study reported that improvements could be made to the currently implemented security strategy. While the IT security professionals' job is to implement security controls using available tools, perform security risk analysis and recommend remediation steps, and assist with the investigation into the root causes of security incidents, including them in security strategy development may improve their attitude, confidence, and ownership in the strategy. Inclusion will lead to improved behavior and security practices whereby heightening the security posture of the organization. The findings from this study may help organizations improve their BYOD security strategy, mitigate the risk of data breach, have better control and oversight over personal mobile devices, propagate cybersecurity knowledge to a larger population, and increased the morale of the IT security professionals tasked with securing the network and data.

IT professionals who are planning to or in the midst of supporting personal devices and implementing a BYOD policy will benefit from this study by learning and comparing the tools that they are currently using with the tools identified in this study and may be able to identify gaps in their own environment and make improvement recommendations. By being directly involved with the design and implementation of the security tools, the intimate knowledge of the tools may improve the efficiency and effectiveness of the IT professional in handling cybersecurity threats and incidents.

Implications for Social Change

The findings from this study contribute to social change by providing organizations that currently or plan to allow personal devices to connect and access information on the business network with data to be used to help improve their security strategy involving BYOD. Since its introduction in 2009 by Intel, the BYOD practice has expanded into different business sectors (Tchao et al., 2017). Numerous K-12 schools across the United States have established BYOD policies allowing students to bring personal mobile devices on campus for learning purposes (Murray, Luo, & Franklin, 2019); while 81% of health care organizations are allowing employees to connect their personal devices to the network to access the electronic health records (EHR) systems (McDermott, Kamerer, & Birk, 2019). The BYOD phenomenon has altered the IT landscape to the point where altering the current security practice and strategy may be necessary.

The consumerization of personal mobile technology is evident at Wi-Fi enable public locations like coffee shops, malls, and fast food restaurants where patrons connect their devices to check e-mail, chat, surf the Internet, and work remotely. The participants in this study declared that even though network security strategies were in place, support for BYOD was weak and that there was room for improvement. Bad actors are constantly looking for opportunities to exploit vulnerabilities and gain access to sensitive data. Organizations that conduct regular security assessments and update their strategies may be more equipped to defend against and reduce cybersecurity risks while individual users will be more vigilant and mindful of the security risks when accessing protected data from their personal devices. IT professionals who are more involved will have more confidence in the tools that they use to maintain and secure the network and computing resources thus affecting their mood and motivation to carry out information security behavior to protect the confidentiality, integrity, and availability of the network environment and the data entrusted to them. Faculty, students, and staff in a university will have a

better appreciation and understanding for IT security and be more accommodating and accepting of policies and security practices put forth by their IT departments. Cooperation from all parties involved will help reduce the amount of damage from cybersecurity threats from the use of BYOD.

Recommendations for Action

In a university environment, students, faculty, staff, and even visitors are connecting their personal network-capable devices, BYOD, to wired and wireless campus networks. While there are strategies currently in place and new policies disseminated, some participants expressed that there is still room for improvement. The university campus network is home to HIPAA, PCI, FERPA, and other protected data that, if compromised, may result in damages to reputation and finance. Not every network environment is equal; care must be considered when evaluating and implementing security strategies. The BYOD phenomenon continues to propagate making every device a potential attack point. The data from this study suggests that the network environment and the tools currently in place may not be enough to secure the data entrusted to and maintained by the institutions.

I recommend that organizations conduct complete analyses of the environments where protected information is housed to identify security gaps and vulnerabilities enabled by the presence of personal mobile devices brought on campus, followed by locating and allocating adequate financial and human resources to support and maintain the security infrastructure to support BYOD. A recent study by Yasin et al. (2018) presented a 5-step approach at validating the organizational security system where the first through third steps are in-line with the above recommendations. In the context of higher education where the main objective is to foster and encourage learning without obstructing progress and exchange of knowledge or invading privacy, the campus security culture may be improved through security policies, training, and public

reminders while access to network data and resources may be improved by using technology that quarantines and blocks suspicious packets and inbound events before it escalates into a security incident.

After receiving CAO approval for this study, the results will be shared to the academic community through the ProQuest database available to students and scholars around the world. I plan on presenting the study and results at security conferences, send a summary to each of the participants, and use the findings as supplemental teaching material to help educate the users within my organization.

Recommendations for Further Study

The BYOD phenomenon has become ubiquitous, occupying education, health care, financial, other corporate business space. The risk associated with the use of personal devices to access private and sensitive data is real. The limitations of this study included the geographical location and the limited timeframe. This study was conducted in California. Other states and countries may have different security requirements, rules, regulations, and governance structures. Repeating the study in a different geographical location may provide additional contrast to this study. This study had to be conducted in a short timeframe to minimize the effects of change to the environment, which would then affect the outcome of the study. Further study may be modified to explore the longitudinal adoption of BYOD from initial consideration through inception then normalcy to establish a deployment framework and timeline.

The context of this study was within the realm of higher education from the IT security professional's perspective. Additional BYOD security research using other business areas like health care, banking, and military where different regulatory security compliances will add to the understanding of managing BYOD organizations and provide contrast to educational institutions.

Reflections

I have worked in the IT field for over 20 years and have witnessed and experienced the incremental changes in technology: from pagers to cellular phones to smartphones; dial-up to ISDN to cable/satellite/DSL to fiber Internet; from 10 MB to 1 GB to over 1 TB local disk storage; and now from hard disk drives (HDD) to solid-state drives (SSD). As an IT professional, security was an integral and implied part of the job; therefore, I did possess a certain degree of bias before conducting this study. However, to ensure that my findings were trustworthy and reliable, I refrained from expressing my opinions and allowed the participants to share their knowledge without coercion by asking open-ended questions and taking inventory of my actions throughout the interviewing process.

While conducting the interviews, I learned how tedious the qualitative process really is. 1) I did not expect that I would have any difficulties recruiting participants, but I did. I had to be persistent in following-up with the gatekeepers to get the names and contacts for the potential participants and then with the potential participants for confirmation of interest in participating; 2) the transcribing process is long and arduous even for a 30-minute recording due to background noise, participants' articulation, and the volume and quality of the recording; and 3) driving from site to site was a tiresome experience. Overall, this experience has been a truly humbling one. Qualitative research requires stamina, dedication, and persistence.

Before embarking on this doctoral journey, I had planned on completing the research study in 4.5 semesters and that all I had to do was recruit participants, conduct interviews, and present my findings; however, I was deeply mistaken and underestimated the degree of work involved. In addition to the research process, I developed a better understanding of the university system that I was a part of and the importance of establishing a balance between security and providing an environment that fosters learning and discovery and that there is not a be-all and

end-all solution to security. Research, regardless of the methods used, contributes to the growing pool of knowledge and I am now exited to begin a new project.

Summary and Study Conclusions

The BYOD phenomenon has grown and become ubiquitous in the university setting. In a university network where each campus has IT autonomy, the tools and policies implemented vary from one campus to another making the managing experience disparate. The decentralized-governance design enables the IT security professionals at each location to explore and decide on the strategies to employ. The strategies and tools currently utilized may not be effective; however, by including the IT security professionals in the development and implementation process, the security strategies can only get better. The BYOD practice brings with it added risks and despite the challenges, the IT security professionals are driven by the desire to help others learn, solve problems, and protect their data.

References

Abate, A., & Krishnaiah, P. (2017). An assessment of the causes and consequences of urban unemployment in small towns of Ethiopia: The case of Sawla Town, SNNPR, Ethiopia. *International Journal of Innovative Research and Development*, *6*(12), 170–179. doi:10.24940/ijird/2017/v6/i12/OCT17091

Abdulkareem, S. A., Augustijn, E.-W., Mustafa, Y. T., & Filatova, T. (2018). Intelligent judgements over health risks in a spatial agent-based model. *International Journal of Health Geographics*, *17*(1), 1–19. doi:10.1186/s12942-018-0128-x

Abdullah, S., Ismail, I., Nor, S. S. M., & Wahab, F. A. (2014). Reliability of knowledge, attitude and practice (KAP) questionnaire on tuberculosis among healthcare workers (HCWs). *International Medical Journal*, *21*(2), 235–238. doi: 10.1037/t40781-000

Abegglen, S., Burns, T., & Sinfield, S. (2016). The power of freedom: Setting up a multimodal exhibition with undergraduate students to foster their learning and help them to achieve. *Journal of Peer Learning*, *9*(1), 1–9. Retrieved from http://ro.uow.edu.au/ajpl/

Adams, G. (2017). Using a narrative approach to illuminate teacher professional learning in an era of accountability. *Teaching and Teacher Education*, *67*, 161–170. doi:10.1016/j.tate.2017.06.007

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In J. Kuhl & J. Beckmann (Eds.), *Action control: From cognition to behavior* (pp. 11–39). doi:10.1007/978-3-642-69746-3_2

Akeju, O., Butakov, S., & Aghili, S. (2018). Main factors and good practices for managing BYOD and IoT risks in a K-12 environment. *International Journal of Internet of Things and Cyber-Assurance*, *1*(1), 22–39. doi:10.1504/ijitca.2018.090161

Alavi, S. S., Dabbagh, S. T., Abbasi, M., & Mehrdad, R. (2017). Medical radiation workers' knowledge, attitude, and practice to protect themselves against ionizing radiation in Tehran Province, Iran. *Journal of Education and Health Promotion*, *6*, 58–65. doi:10.4103/jehp.jehp_126_15

Alftberg, Å., Ahlström, G., Nilsen, P., Behm, L., Sandgren, A., Benzein, E., . . . Rasmussen, B. (2018). Conversations about death and dying with older people: An ethnographic study in nursing homes. *Healthcare*, *6*(2). doi:10.3390/healthcare6020063

Alvinius, A., Johansson, E., & Larsson, G. (2017). Job satisfaction as a form of organizational commitment at the military strategic level: A grounded theory study. *International Journal of Organizational Analysis*, *25*(2), 312–326. doi:10.1108/IJOA-10-2015-0919

Alyahya, M. S., Hijazi, H. H., Al Qudah, J., AlShyab, S., & AlKhalidi, W. (2018). Evaluation of infection prevention and control policies, procedures, and practices: An ethnographic study. *American Journal of Infection Control*, *46*, 1348-1355. doi:10.1016/j.ajic.2018.05.023

Amri, M., Tahir, S. Z. A. B., & Ahmad, S. (2017). The implementation of Islamic teaching in multiculturalism society: A case study at Pesantren schools in

Indonesia. *Asian Social Science*, *13*(6), 125-132. doi:10.5539/ass.v13n6p125

Aramă, C., & Emandii, E. E. (2017). Cryptology and information security. *Scientific Bulletin of Naval Academy*, *2017*(1), 413–419. doi:10.21279/1454-864X-17-I1-067

Arentz, S. (2018). Editorial: Developing intellectual capacity in naturopathy and herbal medicine practice. *Australian Journal of Herbal Medicine*, *30*(1), 6–7. Retrieved from https://nhaa.org.au/publications/australian-journal-of-herbal-medicine

Arpaci, I., Kilicer, K., & Bardakci, S. (2015). Effects of security and privacy concerns on educational use of cloud services. *Computers in Human Behavior*, *45*, 93–98. doi:10.1016/j.chb.2014.11.075

Arseven, I., & Arseven, A. (2014). A study desing using qualitative methods for program evaluation. *International Journal of Academic Research*, *6*(1), 417–422. doi:10.7813/2075-4124.2014/6-1/B.56

Artal, R., & Rubenfeld, S. (2017). Ethical issues in research. *Best Practice & Research: Clinical Obstetrics & Gynaecology*, *43*, 107–114. doi:10.1016/j.bpobgyn.2016.12.006

Badran, H., Pluye, P., & Grad, R. (2015). Advantages and disadvantages of educational email alerts for family physicians: Viewpoint. *Journal of Medical Internet Research*, *17*(2). doi:10.2196/jmir.3773

Balboni, F., Berman, S. J., & Korsten, P. J. (2015). The individual enterprise: All for one and one for all. *Strategy & Leadership*, *43*(4), 3–10. doi:10.1108/sl-05-2015-0034

Ball, J., Hoek, J., Tautolo, E. S., & Gifford, H. (2017). New Zealand policy experts'

appraisal of interventions to reduce smoking in young adults: A qualitative investigation. *BMJ Open*, *7*(12). doi:10.1136/bmjopen-2017-017837

Bann, L. L., Singh, M. M., & Samsudin, A. (2015). Trusted security policies for tackling advanced persistent threat via spear phishing in BYOD environment. *Procedia Computer Science*, *72*, 129–136. doi:10.1016/j.procs.2015.12.113

Barnett, K. B., Livingston, E., Perdue, B., Morgan, P. D., & Fogel, J. (2017). A mixed-method exploratory study of interprofessional education in social work at historically black colleges and universities: A faculty perspective. *Journal of Human Behavior in the Social Environment*, *27*(5), 394–411. doi:10.1080/10911359.2017.1289875

Barnwell, B. J., & Stone, M. H. (2016). Treating high conflict divorce. *Universal Journal of Psychology*, *4*(2), 109–115. doi:10.13189/ujp.2016.040206

Bartolacci, M. R., LeBlanc, L. J., & Podhradsky, A. (2014). Personal denial of service (PDOS) attacks: A discussion and exploration of a new category of cyber crime. *Journal of Digital Forensics, Security and Law*, *9*(1), 19–36. doi:10.15394/jdfsl.2014.1161

Bas, G., & Kivilcim, Z. S. (2017). Teachers' views about educational research: A qualitative study. *International Journal of Progressive Education*, *13*(2), 60–73. Retrieved from http://www.inased.org/ijpe.htm

Bass, M., & Movahed, S. H. (2018). To what extent can 'bring your own device' be an enabler to widening participation in higher education for the socially disadvantaged? *Journal of Perspectives in Applied Academic Practice*, *6*(1), 3–11.

doi:10.14297/jpaap.v6i1.321

Beckett, P. (2018). Focus on protecting what's most important – the data. *Computer Fraud & Security*, *2018*(12), 6–7. doi:10.1016/S1361-3723(18)30118-0

Belak, A., Madarasova Geckova, A., van Dijk, J. P., & Reijneveld, S. A. (2018). Why don't segregated Roma do more for their health? An explanatory framework from an ethnographic study in Slovakia. *International Journal of Public Health*. doi:10.1007/s00038-018-1134-2

Bélanger, F., Collignon, S., Enget, K., & Negangard, E. (2017). Determinants of early conformance with information security policies. *Information & Management*, *54*(7), 887–901. doi:10.1016/j.im.2017.01.003

Bell, S. L., Phoenix, C., Lovell, R., & Wheeler, B. W. (2015). Using GPS and geo-narratives: a methodological approach for understanding and situating everyday green space encounters. *Area*, *47*(1), 88–96. doi:10.1111/area.12152

Bello, A. G., Murray, D., & Armarego, J. (2017). A systematic approach to investigating how information security and privacy can be achieved in BYOD environments. *Information and Computer Security*, *25*(4), 475–492. doi:10.1108/ICS-03-2016-0025

Bennett, S., Dawson, P., Bearman, M., Molloy, E., & Boud, D. (2017). How technology shapes assessment design: Findings from a study of university teachers. *British Journal of Educational Technology*, *48*(2), 672–682. doi:10.1111/bjet.12439

Bishop, A. C., & Cregan, B. R. (2015). Patient safety culture: finding meaning in patient experiences. *International Journal of Health Care Quality Assurance*, *28*(6), 595–

610. doi:10.1108/IJHCQA-03-2014-0029

Blanchard, A. K., Nair, S. G., Bruce, S. G., Ramanaik, S., Thalinja, R., Murthy, S., … Bhattacharjee, P. (2018). A community-based qualitative study on the experience and understandings of intimate partner violence and HIV vulnerability from the perspectives of female sex workers and male intimate partners in North Karnataka state, India. *BMC Women's Health*, *18*(1). doi:10.1186/s12905-018-0554-8

Boehmer, J., LaRose, R., Rifon, N., Alhabash, S., & Cotten, S. (2015). Determinants of online safety behaviour: Towards an intervention strategy for college students. *Behaviour & Information Technology*, *34*(10), 1022–1035. doi:10.1080/0144929X.2015.1028448

Bolkan, S., & Goodboy, A. K. (2016). Rhetorical dissent as an adaptive response to classroom problems: A test of protection motivation theory. *Communication Education*, *65*(1), 24–43. doi:10.1080/03634523.2015.1039557

Bongiovanni, I., Leo, E., Ritrovato, M., Santoro, A., & Derrico, P. (2017). Implementation of best practices for emergency response and recovery at a large hospital: A fire emergency case study. *Safety Science*, *96*, 121–131. doi:10.1016/j.ssci.2017.03.016

Brands, K. M., & Elam, D. A. (2017). Identifying teaching best practices for accounting courses using appreciative inquiry. *International Journal of Knowledge Management Studies*, *8*(1–2), 54–73. doi:10.1504/IJKMS.2017.084412

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. doi:10.1191/1478088706qp063oa

Brook, J., Salmon, D., & Knight, R.-A. (2017). Preparing the sexual health workforce to deliver integrated services: is education the answer? A qualitative study exploring the impact of sexual health education on developing integrated policy and practice. *Primary Health Care Research & Development*, *18*(03), 270–281. doi:10.1017/S1463423617000123

Broom, J. K., Broom, A. F., Kirby, E. R., Gibson, A. F., & Post, J. J. (2017). Clinical and social barriers to antimicrobial stewardship in pulmonary medicine: A qualitative study. *American Journal of Infection Control*, *45*(8), 911–916. doi:10.1016/j.ajic.2017.03.003

Brouwer, N., Heck, A., & Smit, G. (2016). Proctoring to improve teaching practice. *MSOR Connections*, *15*(2), 25. doi:10.21100/msor.v15i2.41

Burns-Sardone, N. (2014). Making the case for BYOD instruction in teacher education. *Issues in Informing Science and Information Technology*, *11*(1), 192–200. doi:10.28945/1988

Byrne, M. M. (2001). Understanding life experiences through a phenomenological approach to research. *AORN Journal*, *73*(4), 830–832. doi:10.1016/S0001-2092(06)61812-7

Cai, D., Kunaviktikul, W., Klunklin, A., Sripusanapan, A., & Avant, P. K. (2017). Identifying the essential components of cultural competence in a Chinese nursing context: A qualitative study: Cultural competence of Chinese nurses. *Nursing & Health Sciences*, *19*(2), 157–162. doi:10.1111/nhs.12308

Campbell, D. J. T., Manns, B. J., Soril, L. J. J., & Clement, F. (2017). Comparison of

Canadian public medication insurance plans and the impact on out-of-pocket costs. *CMAJ Open*, *5*(4), E808–E813. doi:10.9778/cmajo.20170065

Cardoni, A., Dumay, J., Palmaccio, M., & Celenza, D. (2018). Knowledge transfer in a start-up craft brewery. *Business Process Management Journal*. doi:10.1108/BPMJ-07-2017-0205

Cascardo, D. (2016). Insights into cyber security risks: The key to survival is resiliency. *Journal of Medical Practice Management*, *32*(3), 169–172. Retrieved from https://greenbranch.com/store/index.cfm/category/31/the-mpm-journal.cfm

Cebrián, G. (2017). A collaborative action research project towards embedding ESD within the higher education curriculum. *International Journal of Sustainability in Higher Education*, *18*(6), 857–876. doi:10.1108/IJSHE-02-2016-0038

Chen, H., Beaudoin, C. E., & Hong, T. (2016). Protecting oneself online: The effects of negative privacy experiences on privacy protective behaviors. *Journalism & Mass Communication Quarterly*, *93*(2), 409–429. doi:10.1177/1077699016640224

Chen, H., Beaudoin, C. E., & Hong, T. (2017). Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors. *Computers in Human Behavior*, *70*, 291–302. doi:10.1016/j.chb.2017.01.003

Chen, H., Wang, X., Li, Z., Chen, W., & Cai, Y. (2019). Distributed sensing and cooperative estimation/detection of ubiquitous power internet of things. *Protection and Control of Modern Power Systems*, *4*(1). doi:10.1186/s41601-019-0128-2

Chen, J., & Li, C. (2018). Research on meteorological information network security system based on VPN technology. *MATEC Web of Conferences*, *232*, 01001–01004. doi:10.1051/matecconf/201823201001

Chen, Y., & Zahedi, F. M. (2016). Individuals' internet security perceptions and behaviors: Polycontextual contrasts between the United States and China. *MIS Quarterly*, *40*(1), 205-A12. doi:10.25300/MISQ/2016/40.1.09

Cheng, G., Guan, Y., & Chau, J. (2016). An empirical study towards understanding user acceptance of bring your own device (BYOD) in higher education. *Australasian Journal of Educational Technology*, *32*(4). doi:10.14742/ajet.2792

Cho, V., & Ip, W. H. (2018). A study of BYOD adoption from the lens of threat and coping appraisal of its security policy. *Enterprise Information Systems*, *12*(6), 659–673. doi:10.1080/17517575.2017.1404132

Chou, H.-L., & Chou, C. (2016). An analysis of multiple factors relating to teachers' problematic information security behavior. *Computers in Human Behavior*, *65*, 334–345. doi:10.1016/j.chb.2016.08.034

Chou, P.-N., Chang, C.-C., & Lin, C.-H. (2017). BYOD or not: A comparison of two assessment strategies for student learning. *Computers in Human Behavior*, *74*, 63–71. doi:10.1016/j.chb.2017.04.024

Chow, L. P. (1968). A study on the demographic impact of an IUD programme. *Population Studies*, *22*(3), 347–359. doi:10.2307/2173000

Chu, A. M. Y., Chau, P. Y. K., & So, M. K. P. (2015). Explaining the misuse of information systems resources in the workplace: A dual-process approach.

Journal of Business Ethics, *131*(1), 209–225. doi:10.1007/s10551-014-2250-4

Chung, M. (2019). Why employees matter in the fight against ransomware. *Computer Fraud & Security*, *2019*(8), 8–11. doi:10.1016/S1361-3723(19)30084-3

Clandinin, D. J., Cave, M. T., & Berendonk, C. (2017). Narrative inquiry: A relational research methodology for medical education. *Medical Education*, *51*(1), 89–96. doi:10.1111/medu.13136

Clayton, A. B., Medina, M. C., & Wiseman, A. M. (2017). Culture and community: Perspectives from first-year, first-generation-in-college Latino students. *Journal of Latinos and Education*, 1–17. doi:10.1080/15348431.2017.1386101

Clubb, A. C., & Hinkle, J. C. (2015). Protection motivation theory as a theoretical framework for understanding the use of protective measures. *Criminal Justice Studies*, *28*(3), 336–355. doi:10.1080/1478601X.2015.1050590

Colder Carras, M., Kalbarczyk, A., Wells, K., Banks, J., Kowert, R., Gillespie, C., & Latkin, C. (2018). Connection, meaning, and distraction: A qualitative study of video game play and mental health recovery in veterans treated for mental and/or behavioral health problems. *Social Science & Medicine*. doi:10.1016/j.socscimed.2018.08.044

Colorafi, K. J., & Evans, B. (2016). Qualitative descriptive methods in health science research. *HERD*, *9*(4), 16–25. doi:10.1177/1937586715614171

Cooper, S., Leon, N., Namadingo, H., Bobrow, K., & Farmer, A. J. (2018). “My wife’s mistrust. That’s the saddest part of being a diabetic”: A qualitative study of sexual well-being in men with type 2 diabetes in sub-Saharan Africa. *PLoS One*, *13*(9).

doi:10.1371/journal.pone.0202413

Cope, D. (2015). Case study research methodology in nursing research. *Oncology Nursing Forum*, *42*(6), 681–682. doi:10.1188/15.ONF.681-682

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2017). Organizational information security policies: a review and research framework. *European Journal of Information Systems*, *26*(6), 605–641. doi:10.1057/s41303-017-0059-9

Crampton, A. (2016). Escape from the laboratory: Ethnographic methods in the study of elder and family court mediation. *Negotiation Journal*, *32*(3), 191–211. doi:10.1111/nejo.12155

Crossler, R. E., Long, J. H., Loraas, T. M., & Trinkle, B. S. (2014). Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-behavior gap. *Journal of Information Systems*, *28*(1), 209–226. doi:10.2308/isys-50704

Cunningham, J. A., Menter, M., & Young, C. (2017). A review of qualitative case methods trends and themes used in technology transfer research. *The Journal of Technology Transfer*, *42*(4), 923–956. doi:10.1007/s10961-016-9491-6

Curnalia, R. M. L., & Mermer, D. (2018). Renewing our commitment to tenure, academic freedom, and shared governance to navigate challenges in higher education. *Review of Communication*, *18*(2), 129–139. doi:10.1080/15358593.2018.1438645

Dadzie, G., Aziato, L., & Aikins, A. d.-G. (2017). "We are the best to stand in for patients": a qualitative study on nurses' advocacy characteristics in Ghana. *BMC Nursing*, *16*(1). doi:10.1186/s12912-017-0259-6

Dahl, K., Larivière, N., & Corbière, M. (2017). Work participation of individuals with borderline personality disorder: A multiple case study. *Journal of Vocational Rehabilitation*, *46*(3), 377–388. doi:10.3233/JVR-170874

Daneshkohan, A., Hosseinzadeh, M., Abolfathi, R., Hekmatifar, A., & Bajalanlou, F. (2015). Study of knowledge, attitudes and practice towards the Internet among BSc students of school of public health, Shahid Beheshti University of Medical Sciences. *Journal of Medical Education*, *14*(3), 93–98. doi:10.22037/jme.v14i3.10255

Dang-Pham, D., & Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach. *Computers & Security*, *48*(Supplement C), 281–297. doi:10.1016/j.cose.2014.11.002

Davidson, J. W., McNamara, B., Rosenwax, L., Lange, A., Jenkins, S., & Lewin, G. (2014). Evaluating the potential of group singing to enhance the well-being of older people. *Australasian Journal on Ageing*, *33*(2), 99–104. doi:10.1111/j.1741-6612.2012.00645.x

Davis, S. M., Davidov, D., Kristjansson, A. L., Zullig, K., Baus, A., & Fisher, M. (2018). Qualitative case study of needle exchange programs in the Central Appalachian region of the United States. *PLoS One*, *13*(10). doi:10.1371/journal.pone.0205466

de Bont, E. G., Francis, N. A., Dinant, G.-J., & Cals, J. W. (2014). Parents' knowledge, attitudes, and practice in childhood fever: an internet-based survey. *British*

Journal of General Practice, *64*(618), e10–e16. doi:10.3399/bjgp14X676401

Denedo, M., Thomson, I., & Yonekura, A. (2018). Ecological damage, human rights and oil: Local advocacy NGOs dialogic action and alternative accounting practices. *Accounting Forum*. doi:10.1016/j.accfor.2018.09.001

Deng, Q., Ma, Y., & Li, M. (2016). Research on one to one digital learning mode based on BYOD. *Journal of Residuals Science & Technology*, *13*(7). doi:10.12783/issn.1544-8053/13/7/176

Doane, A. N., Boothe, L. G., Pearson, M. R., & Kelley, M. L. (2016). Risky electronic communication behaviors and cyberbullying victimization: An application of protection motivation theory. *Computers in Human Behavior*, *60*, 508–513. doi:10.1016/j.chb.2016.02.010

Dörnyei, K. R., & Gyulavári, T. (2016). Why do not you read the label? - an integrated framework of consumer label information search. *International Journal of Consumer Studies*, *40*(1), 92–100. doi:10.1111/ijcs.12218

Dragojevic, M., Savage, M. W., Scott, A. M., & McGinnis, T. (2018). Promoting oral health in Appalachia: Effects of threat label and source accent on message acceptance. *Health Communication*, 1–11. doi:10.1080/10410236.2018.1560581

Durodola, O., Fusch, P., & Tippins, S. (2017). A case-study of financial literacy and wellbeing of immigrants in Lloydminster, Canada. *International Journal of Business and Management*, *12*(8), 37–50. doi:10.5539/ijbm.v12n8p37

Durosaiye, I. O., Hadjri, K., Liyanage, C. L., & Bennett, K. (2018). A matrix for the qualitative evaluation of nursing tasks. *Journal of Nursing Management*, *26*(3),

274–287. doi:10.1111/jonm.12543

Elaoud, A., & Jarboui, A. (2017). Auditor specialization, accounting information quality and investment efficiency. *Research in International Business and Finance*, *42*, 616–629. doi:10.1016/j.ribaf.2017.07.006

Ellwanger, G., Runge, S., Wagner, M., Ackermann, W., Neukirchen, M., Frederking, W., … Sukopp, U. (2018). Current status of habitat monitoring in the European Union according to Article 17 of the Habitats Directive, with an emphasis on habitat structure and functions and on Germany. *Nature Conservation*, *29*, 57–78. doi:10.3897/natureconservation.29.27273

Ennis, L., Ablett, J., Taylor, M., & Lal, S. (2018). The active problem solving of patients dependent on home parenteral nutrition: A qualitative analysis. *Clinical Nutrition ESPEN*, *26*, 77–83. doi:10.1016/j.clnesp.2018.04.010

Eshtaiwi, M., Badi, I., Abdulshahed, A., & Erkan, T. E. (2018). Determination of key performance indicators for measuring airport success: A case study in Libya. *Journal of Air Transport Management*, *68*, 28–34. doi:10.1016/j.jairtraman.2017.12.004

Farai, M., & Mugove, K. (2017). Love in the office and along the corridors: causes and consequences: A case study of a beverage firm in Zimbabwe. *Journal of Social Sciences*, *51*(1–3), 179–198. doi:10.1080/09718923.2017.1305556

Farooq, M. B., & de Villiers, C. (2017). Telephonic qualitative research interviews: when to consider them and how to do them. *Meditari Accountancy Research*, *25*(2), 291–316. doi:10.1108/MEDAR-10-2016-0083

Farooqui, M., Yahaya, B., Hussien, A., & Farooqui, M. (2016). Knowledge, attitude and practice (KAP) regarding blood donation among health care workers in Malaysia. *Value in Health*, *19*(7), A828. doi:10.1016/j.jval.2016.08.593

Flax, V. L., Hamela, G., Mofolo, I., Hosseinipour, M. C., Hoffman, I. F., & Maman, S. (2017). Factors influencing postnatal Option B+ participation and breastfeeding duration among HIV-positive women in Lilongwe District, Malawi: A qualitative study. *PLoS One*, *12*(4). doi:10.1371/journal.pone.0175590

Foltz, C. B., Newkirk, H. E., & Schwager, P. H. (2016). An empirical investigation of factors that influence individual behavior toward changing social networking security settings. *Journal of Theoretical and Applied Electronic Commerce Research*, *11*(2), 2–2. doi:10.4067/S0718-18762016000200002

Fox, A. [Alexa] K., Bacile, T. J., Nakhata, C., & Weible, A. (2018). Selfie-marketing: Exploring narcissism and self-concept in visual user-generated content on social media. *Journal of Consumer Marketing*, *35*(1), 11–21. doi:10.1108/JCM-03-2016-1752

Fox, A. [Amanda], Gardner, G., & Osborne, S. (2018). Nursing service innovation: A case study examining emergency nurse practitioner service sustainability. *Journal of Advanced Nursing*, *74*(2), 454–464. doi:10.1111/jan.13454

French, A. M., Guo, C., & Shim, J. P. (2014). Current status, issues, and future of bring your own device (BYOD). *Communications of the Association for Information Systems*, *35*, 191–197. doi:10.17705/1cais.03510

Fugard, A. J. B., & Potts, H. W. W. (2015). Supporting thinking on sample sizes for

thematic analyses: a quantitative tool. *International Journal of Social Research Methodology*, *18*(6), 669–684. doi:10.1080/13645579.2015.1005453

Gao, Y., Li, H., & Luo, Y. (2015). An empirical study of wearable technology acceptance in healthcare. *Industrial Management & Data Systems*, *115*(9), 1704–1723. doi:10.1108/IMDS-03-2015-0087

Garba, A. B., Armarego, J., & Murray, D. (2015). Bring your own device organizational information security and privacy. *ARPN Journal of Engineering and Applied Sciences*, *10*(3), 1279–1287. Retrieved from http://www.arpnjournals.com/jeas/

Genga, E. K., Achieng, L., Njiri, F., & Ezzi, M. S. (2017). Knowledge, attitudes, and practice survey about antimicrobial resistance and prescribing among physicians in a hospital setting in Nairobi, Kenya. *African Journal of Respiratory Medicine*, *12*(2), 3–7. Retrieved from http://www.africanjournalofrespiratorymedicine.com/

Ghaemi Rad, T., Sadeghi-Niaraki, A., Abbasi, A., & Choi, S.-M. (2018). A methodological framework for assessment of ubiquitous cities using ANP and DEMATEL methods. *Sustainable Cities and Society*, *37*, 608–618. doi:10.1016/j.scs.2017.11.024

Gibson, C. B. (2016). Elaboration, generalization, triangulation, and interpretation: On enhancing the value of mixed method research. *Organizational Research Methods*, *20*(2), 193–223. doi:10.1177/1094428116639133

Giedraitis, A., Stašys, R., & Skirpstaitė, R. (2017). Management team development opportunities: A case of Lithuanian furniture company. *Entrepreneurship and Sustainability Issues*, *5*(2), 212–222. doi:10.9770/jesi.2017.5.2(4)

Gillies, C. G. M. (2016). To BYOD or not to BYOD: Factors affecting academic acceptance of student mobile devices in the classroom. *Research in Learning Technology*, *24*. doi:10.3402/rlt.v24.30357

Goldstone, D., & Bantjes, J. (2017). Mental health care providers' perceptions of the barriers to suicide prevention amongst people with substance use disorders in South Africa: a qualitative study. *International Journal of Mental Health Systems*, *11*(1). doi:10.1186/s13033-017-0153-3

Gorniewicz, J., Floyd, M., Krishnan, K., Bishop, T. W., Tudiver, F., & Lang, F. (2017). Breaking bad news to patients with cancer: A randomized control trial of a brief communication skills training module incorporating the stories and preferences of actual patients. *Patient Education and Counseling*, *100*(4), 655–666. doi:10.1016/j.pec.2016.11.008

Grossoehme, D. H. (2014). Overview of qualitative research. *Journal of Health Care Chaplaincy*, *20*(3), 109–122. doi:10.1080/08854726.2014.925660

Guba, E. G., & Lincoln, Y. S. (1994). Competing paradigms in qualitative research. In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of qualitative research* (pp. 105–117). Thousand Oaks, CA: Sage.

Gustafsson, I., Nyström, M., & Palmér, L. (2017). Midwives' lived experience of caring for new mothers with initial breastfeeding difficulties: A phenomenological study. *Sexual & Reproductive Healthcare*, *12*, 9–15. doi:10.1016/j.srhc.2016.12.003

Gutiérrez-Porlán, I., Román-García, M., & Sánchez-Vera, M.-M. (2018). Strategies for the communication and collaborative online work by university students.

Comunicar, *26*(54), 91–99. doi:10.3916/C54-2018-09

Ha, L., & Pepin, J. (2018). Clinical nursing leadership educational intervention for first-year nursing students: A qualitative evaluation. *Nurse Education in Practice*, *32*, 37–43. doi:10.1016/j.nepr.2018.07.005

Halcomb, E., & Peters, K. (2016). Research would not be possible without participants. *Nurse Researcher*, *24*(1), 6. doi:10.7748/nr.24.1.6.s2

Hamilton, C. B., Hoens, A. M., Backman, C. L., McKinnon, A. M., McQuitty, S., English, K., & Li, L. C. (2018). An empirically based conceptual framework for fostering meaningful patient engagement in research. *Health Expectations*, *21*(1), 396–406. doi:10.1111/hex.12635

Hanus, B., Windsor, J. C., & Wu, Y. (2018). Definition and multidimensionality of security awareness: Close encounters of the second order. *The Data Base for Advances in Information Systems*, *49*(SI), 103–132. doi:10.1145/3210530.3210538

Hanus, B., & Wu, Y. (2016). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management*, *33*(1), 2–16. doi:10.1080/10580530.2015.1117842

Happa, J., Glencross, M., & Steed, A. (2019). Cyber security threats and challenges in collaborative mixed-reality. *Frontiers in ICT*, *6*. doi:10.3389/fict.2019.00005

Harding, K. E., Robertson, N., Snowdon, D. A., Watts, J. J., Karimi, L., O'Reilly, M., … Taylor, N. F. (2018). Are wait lists inevitable in subacute ambulatory and community health services? A qualitative analysis. *Australian Health Review*,

42(1), 93-99. doi:10.1071/AH16145

Harrison, A., Burress, R., Velasquez, S., & Schreiner, L. (2017). Social media use in academic libraries: A phenomenological study. *The Journal of Academic Librarianship*, *43*(3), 248–256. doi:10.1016/j.acalib.2017.02.014

Haude, K., McCarthy Veach, P., LeRoy, B., & Zierhut, H. (2017). Factors influencing the decision-making process and long-term interpersonal outcomes for parents who undergo preimplantation genetic diagnosis for Fanconi Anemia: A qualitative investigation. *Journal of Genetic Counseling*, *26*(3), 640–655. doi:10.1007/s10897-016-0032-0

Henningsen, M. J., Sort, R., Møller, A. M., & Herling, S. F. (2018). Peripheral nerve block in ankle fracture surgery: a qualitative study of patients' experiences. *Anaesthesia*, *73*(1), 49–58. doi:10.1111/anae.14088

Henson, A. (2017). Strengthening evaluation research: A case study of an evaluability assessment conducted in a carceral setting. *International Journal of Offender Therapy and Comparative Criminology*, 1–17. doi:10.1177/0306624X17723641

Holton, G., Joyner, K., & Mash, B. (2018). Sexual assault survivors' perspectives on clinical follow-up in the Eden District, South Africa: A qualitative study. *African Journal of Primary Health Care & Family Medicine*, *10*(1). doi:10.4102/phcfm.v10i1.1631

Houghton, C., Casey, D., & Smyth, S. (2017). Selection, collection and analysis as sources of evidence in case study research. *Nurse Researcher*, *24*(4), 36–41. doi:10.7748/nr.2017.e1482

Houghton, C., Murphy, K., Shaw, D., & Casey, D. (2015). Qualitative case study data analysis: an example from practice. *Nurse Researcher*, *22*(5), 8–12. doi:10.7748/nr.22.5.8.e1307

Huijnen, C. A. G. J., Lexis, M. A. S., Jansens, R., & de Witte, L. P. (2017). How to Implement Robots in Interventions for Children with Autism? A Co-creation Study Involving People with Autism, Parents and Professionals. *Journal of Autism and Developmental Disorders*, *47*(10), 3079–3096. doi:10.1007/s10803-017-3235-9

Hung, H.-T. (2017). Clickers in the flipped classroom: Bring your own device (BYOD) to promote student learning. *Interactive Learning Environments*, *25*(8), 983–995. doi:10.1080/10494820.2016.1240090

Inauen, J., & Mosler, H.-J. (2016). Mechanisms of behavioural maintenance: Long-term effects of theory-based interventions to promote safe water consumption. *Psychology & Health*, *31*(2), 166–183. doi:10.1080/08870446.2015.1085985

Ippolito, M., Chary, A., Daniel, M., Barnoya, J., Monroe, A., & Eakin, M. (2017). Expectations of health care quality among rural Maya villagers in Sololá Department, Guatemala: A qualitative analysis. *International Journal for Equity in Health*, *16*(1). doi:10.1186/s12939-017-0547-5

Ismail, K. A., Singh, M. M., Mustaffa, N., Keikhosrokiani, P., & Zulkefli, Z. (2017). Security strategies for hindering watering hole cyber crime attack. *Procedia Computer Science*, *124*, 656–663. doi:10.1016/j.procs.2017.12.202

Jackman, P. C., Crust, L., & Swann, C. (2017). Systematically comparing methods used

to study flow in sport: A longitudinal multiple-case study. *Psychology of Sport and Exercise*, *32*, 113–123. doi:10.1016/j.psychsport.2017.06.009

Jackson, C., Snyder, J., Crooks, V. A., & Lavergne, M. R. (2018). "I didn't have to prove to anybody that I was a good candidate": A case study framing international bariatric tourism by Canadians as circumvention tourism. *BMC Health Services Research*, *18*(1). doi:10.1186/s12913-018-3385-2

Jafarkarimi, H., Saadatdoost, R., Sim, A. T. H., & Hee, J. M. (2016). Behavioral intention in social networking sites ethical dilemmas: An extended model based on Theory of Planned Behavior. *Computers in Human Behavior*, *62*, 545–561. doi:10.1016/j.chb.2016.04.024

Jansen, J., & Leukfeldt, R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. *International Journal of Cyber Criminology*, *10*(1), 79–91. doi:10.528 1/zenodo.58523

Jansen, J., Veenstra, S., Zuurveen, R., & Stol, W. (2016). Guarding against online threats: why entrepreneurs take protective measures. *Behaviour & Information Technology*, *35*(5), 368–379. doi:10.1080/0144929X.2016.1160287

Jansen van Rensburg, J. M., Maree, J., & Casteleijn, D. (2017). An investigation into the quality of life of cancer patients in South Africa. *Asia-Pacific Journal of Oncology Nursing*, *4*(4), 336–341. doi:10.4103/apjon.apjon_41_17

Jaskiewicz, P., Combs, J. G., & Rau, S. B. (2015). Entrepreneurial legacy: Toward a theory of how some family firms nurture transgenerational entrepreneurship.

Journal of Business Venturing, *30*(1), 29–49. doi:10.1016/j.jbusvent.2014.07.001

Jenness, V., & Calavita, K. (2017). Prisoner grievances, rights, and the culture of control. *Ohio State Journal of Criminal Law*, *15*(1), 211–228. doi:10.1111/lasr.12312

Jervis, M. G., & Drake, M. A. (2014). The use of qualitative research methods in quantitative science: A review. *Journal of Sensory Studies*, *29*(4), 234–247. doi:10.1111/joss.12101

Jiang, M., Tsai, H. S., Cotten, S. R., Rifon, N. J., LaRose, R., & Alhabash, S. (2016). Generational differences in online safety perceptions, knowledge, and practices. *Educational Gerontology*, *42*(9), 621–634. doi:10.1080/03601277.2016.1205408

Johnson, E., & Menna, R. (2017). Help seeking among adolescents in foster care: A qualitative study. *Children and Youth Services Review*, *76*, 92–99. doi:10.1016/j.childyouth.2017.03.002

Kadam, R. A. (2017). Informed consent process: A step further towards making it meaningful! *Perspectives in Clinical Research*, *8*(3), 107–112. doi:10.4103/picr.PICR_147_16

Kadimo, K., Kebaetse, M. B., Ketshogileng, D., Seru, L. E., Sebina, K. B., Kovarik, C., & Balotlegi, K. (2018). Bring-your-own-device in medical schools and healthcare facilities: A review of the literature. *International Journal of Medical Informatics*, *119*, 94–102. doi:10.1016/j.ijmedinf.2018.09.013

Kallio, H., Pietilä, A.-M., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. *Journal of Advanced Nursing*, *72*(12), 2954–2965.

doi:10.1111/jan.13031

Kalmakis, K. A., Chandler, G. E., Roberts, S. J., & Leung, K. (2017). Nurse practitioner screening for childhood adversity among adult primary care patients: A mixed-method study. *Journal of the American Association of Nurse Practitioners*, *29*(1), 35–45. doi:10.1002/2327-6924.12378

Kang, J., & Jeong, Y. J. (2018). Embracing the new vulnerable self: A grounded theory approach on critical care survivors' post-intensive care syndrome. *Intensive and Critical Care Nursing*. doi:10.1016/j.iccn.2018.08.004

Kaspar, K. (2015). An embodiment perspective on protection motivation theory: The impact of incidental weight sensations on threat-appraisal, coping-appraisal, and protection motivation. *Studia Psychologica*, *57*(4), 301–314. doi:10.21909/sp.2015.03.701

Kattoor, A., Thomas, J., Abraham, A., Bahia, A., & Kenchaiah, S. (2017). Tobacco cessation: A knowledge, attitude and practice (KAP) survey among residents. *Journal of the American College of Cardiology*, *69*(11), 2529. doi:10.1016/S0735-1097(17)35918-1

Kaur, H. (2016). Technology transforming mathematics education. *International Journal of Advanced Research in Computer Science*, *7*(6), 246–249. Retrieved from http://www.ijarcs.info/

Kay, R., Benzimra, D., & Li, J. (2017). Exploring factors that influence technology-based distractions in bring your own device classrooms. *Journal of Educational Computing Research*, *55*(7), 974–995. doi:10.1177/0735633117690004

Kebede, A., Retta, N., Abuye, C., & Malde, M. (2016). Community knowledge, attitude and practices (KAP) on fluorosis and its mitigation in endemic areas of Ethiopia. *African Journal of Food, Agriculture, Nutrition and Development*, *16*(1), 10715–10726. doi:10.18697/ajfand.73.15480

Khan, Y., Sarriff, A., Khan, A., & Mallhi, T. (2014). Knowledge, attitude and practice (KAP) survey of osteoporosis among students of a tertiary institution in Malaysia. *Tropical Journal of Pharmaceutical Research*, *13*(1), 155. doi:10.4314/tjpr.v13i1.22

Kim, S. S., & Kim, Y. J. (2017). The effect of compliance knowledge and compliance support systems on information security compliance behavior. *Journal of Knowledge Management*, *21*(4), 986–1010. doi:10.1108/JKM-08-2016-0353

Kodadek, L. M., Kapadia, M. R., Changoor, N. R., Dunn, K. B., Are, C., Greenberg, J. A., … Haider, A. H. (2016). Educating the surgeon-scientist: A qualitative study evaluating challenges and barriers toward becoming an academically successful surgeon. *Surgery*, *160*(6), 1456–1465. doi:10.1016/j.surg.2016.07.003

Kooij, L., Groen, W. G., & van Harten, W. H. (2018). Barriers and facilitators affecting patient portal implementation from an organizational perspective: qualitative study. *Journal of Medical Internet Research*, *20*(5). doi:10.2196/jmir.8989

Korstjens, I., & Moser, A. (2018). Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing. *European Journal of General Practice*, *24*(1), 120–124. doi:10.1080/13814788.2017.1375092

Kossover-Smith, R. A., Coutts, K., Hatfield, K. M., Cochran, R., Akselrod, H., Schaefer,

M. K., … Bruss, K. (2017). One needle, one syringe, only one time? A survey of physician and nurse knowledge, attitudes, and practices around injection safety. *American Journal of Infection Control*, *45*(9), 1018–1023. doi:10.1016/j.ajic.2017.04.292

Kostov, C. E., Rees, C. E., Gormley, G. J., & Monrouxe, L. V. (2018). 'I did try and point out about his dignity': A qualitative narrative study of patients and carers' experiences and expectations of junior doctors. *BMJ Open*, *8*(1), e017738–e017751. doi:10.1136/bmjopen-2017-017738

Kruth, J. G. (2015). Five qualitative research approaches and their applications in parapsychology. *The Journal of Parapsychology*, *79*(2), 219–233. Retrieved from http://www.rhine.org/what-we-do/journal-of-parapsychology.html

Kumar, R., Zarour, M., Alenezi, M., Agrawal, A., & Khan, R. A. (2019). Measuring security durability of software through fuzzy-based decision-making process. *International Journal of Computational Intelligence Systems*, *12*(2), 627–642. doi:10.2991/ijcis.d.190513.001

Largent, E. A., & Lynch, H. F. (2017). Paying research participants: regulatory uncertainty, conceptual confusion, and a path forward. *Yale Journal of Health Policy, Law, and Ethics*, *17*(1), 61–141. Retrieved from http://www.law.yale.edu/academics/yjhple.htm

Lee, J., Warkentin, M., Crossler, R. E., & Otondo, R. F. (2017). Implications of monitoring mechanisms on bring your own device adoption. *Journal of Computer Information Systems*, *57*(4), 309–318. doi:10.1080/08874417.2016.1184032

Lewis, S. R. (2017). The practice of health program evaluation. *Health Promotion Practice*, *18*(6), 782–784. doi:10.1177/1524839917711185

Li, D., Gao, Q., Liu, J., Feng, Y., Ning, W., Dong, Y., … Xin, D. (2015). Knowledge, attitude, and practices (KAP) and risk factors analysis related to cystic echinococcosis among residents in Tibetan communities, Xiahe County, Gansu Province, China. *Acta Tropica*, *147*, 17–22. doi:10.1016/j.actatropica.2015.02.018

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13–24. doi:10.1016/j.ijinfomgt.2018.10.017

Li, R., Xie, R., Yang, C., Rainey, J., Song, Y., & Greene, C. (2018). Identifying ways to increase seasonal influenza vaccine uptake among pregnant women in China: A qualitative investigation of pregnant women and their obstetricians. *Vaccine*, *36*(23), 3315–3322. doi:10.1016/j.vaccine.2018.04.060

Limba, T., Plėta, T., Agafonov, K., & Damkus, M. (2017). Cyber security management model for critical infrastructure. *Entrepreneurship and Sustainability Issues*, *4*(4), 559–573. doi:10.9770/jesi.2017.4.4(12)

Liu, L., Chen, W. P., Solanas, A., & He, A. L. (2017). Knowledge, attitude, and practice about internet of things for healthcare. In *2017 International Smart Cities Conference (ISC2)* (pp. 1–4). doi:10.1109/ISC2.2017.8090829

Love, J., & Tuokko, H. (2016). Older driver safety: A survey of psychologists' attitudes, knowledge, and practices. *Canadian Journal on Aging*, *35*(3), 393–404.

doi:10.1017/S0714980816000386

Luctkar-Flude, M., Tyerman, J., & Groll, D. (2018). Exploring the use of neurofeedback by cancer survivors: Results of interviews with neurofeedback providers and clients. *Asia-Pacific Journal of Oncology Nursing*. doi:doi:10.4103/apjon.apjon_34_18

Luor, T., Lu, H.-P., Yu, H., & Lu, Y. (2015). Exploring the critical quality attributes and models of smart homes. *Maturitas*, *82*(4), 377–386. doi:10.1016/j.maturitas.2015.07.025

Lusk, J., Dobscha, S. K., Kopacz, M., Ritchie, M. F., & Ono, S. (2018). Spirituality, Religion, and Suicidality Among Veterans: A Qualitative Study. *Archives of Suicide Research*, *22*(2), 311–326. doi:10.1080/13811118.2017.1340856

Lysaght, R., Krupa, T., Kranenburg, R., & Armstrong, C. (2016). Participant recruitment for studies on disability and work: Challenges and solutions. *Journal of Occupational Rehabilitation*, *26*(2), 125–140. doi:10.1007/s10926-015-9594-1

MacLure, K., & Stewart, D. (2018). A qualitative case study of ehealth and digital literacy experiences of pharmacy staff. *Research in Social and Administrative Pharmacy*, *14*(6), 555–563. doi:10.1016/j.sapharm.2017.07.001

Madar, R., Adini, B., Greenberg, D., Waisman, Y., & Goldberg, A. (2018). Perspectives of health professionals on the best care settings for pediatric trauma casualties: a qualitative study. *Israel Journal of Health Policy Research*, *7*(1). doi:10.1186/s13584-018-0207-2

Madhwani, K., & Nag, P. (2017). Web-based kap intervention on office ergonomics: A

unique technique for prevention of musculoskeletal discomfort in global corporate offices. *Indian Journal of Occupational and Environmental Medicine*, *21*(1), 18. doi:10.4103/ijoem.IJOEM_145_17

Magnan, R. E., Shorey Fennell, B. R., & Brady, J. M. (2017). Health decision making and behavior: The role of affect-laden constructs. *Social and Personality Psychology Compass*, *11*(8), e12333. doi:10.1111/spc3.12333

Magruder, J. S., Lewis, S. X., Burks, E. J., & Smolinski, C. (2015). Bring your own device (BYOD)--Who is running organizations? *Journal of Accounting and Finance*, *15*(1), 55–61. Retrieved from http://www.na-businesspress.com/jafopen.html

Maimon, D., Kamerdze, A., Cukier, M., & Sobesto, B. (2013). Daily trends and origin of computer-focused crimes against a large university computer network: An application of the routine-activities and lifestyle perspective. *The British Journal of Criminology*, *53*(2), 319–343. doi:10.1093/bjc/azs067

Makarovs, K., & Achterberg, P. (2017). Contextualizing educational differences in "vaccination uptake": A thirty nation survey. *Social Science & Medicine*, *188*, 1–10. doi:10.1016/j.socscimed.2017.06.039

Mammen, B., Hills, D. J., & Lam, L. (2018). Newly qualified graduate nurses' experiences of workplace incivility in Australian hospital settings. *Collegian*, 1–9. doi:10.1016/j.colegn.2018.08.003

Manera, K. E., Craig, J. C., Johnson, D. W., & Tong, A. (2018). The power of the patient voice: Conducting and using qualitative research to improve care and outcomes in

peritoneal dialysis. *Peritoneal Dialysis International*, *38*(4), 242–245. doi:10.3747/pdi.2017.00280

Martens, M., De Wolf, R., & De Marez, L. (2019). Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. *Computers in Human Behavior*, *92*, 139–150. doi:10.1016/j.chb.2018.11.002

Martin, G. P., Aveling, E.-L., Campbell, A., Tarrant, C., Pronovost, P. J., Mitchell, I., … Dixon-Woods, M. (2018). Making soft intelligence hard: a multi-site qualitative study of challenges relating to voice about safety concerns. *BMJ Quality & Safety*, *27*(9), 710–717. doi:10.1136/bmjqs-2017-007579

Ma'ruf, K. F., & Rochman, M. M. (2019). Guidelines for developing information security training and awareness programs in government agency: The perspective of ADDIE instructional design models (a case study in Indonesian government agency). *People: International Journal of Social Sciences*, *5*(2), 863–877. doi:10.20319/pijss.2019.52.863877

Mazerolle, S. M., Myers, S. L., Walker, S. E., & Kirby, J. (2018). Maintaining professional commitment as a newly credentialed athletic trainer in the secondary school setting. *Journal of Athletic Training*, *53*(3), 312–319. doi:10.4085/1062-6050-72-17

Mazloomy, S. S., Baghianimoghadam, M. H., Ehrampoush, M. H., Baghianimoghadam, B., Mazidi, M., & Mozayan, M. R. (2014). A study of the knowledge, attitudes, and practices (KAP) of the women referred to health centers for cardiovascular

disease (CVDs) and their risk factors. *Health Care for Women International*, *35*(1), 50–59. doi:10.1080/07399332.2012.755980

McCusker, K., & Gunaydin, S. (2015). Research using qualitative, quantitative or mixed methods and choice based on the research. *Perfusion*, *30*(7), 537–542. doi:10.1177/0267659114559116

McDermott, D. S., Kamerer, J. L., & Birk, A. T. (2019). Electronic health records: A literature review of cyber threats and security measures. *International Journal of Cyber Research and Education*, *1*(2), 42–49. doi:10.4018/IJCRE.2019070104

McGrath, C., Palmgren, P. J., & Liljedahl, M. (2018). Twelve tips for conducting qualitative research interviews. *Medical Teacher*, 1–5. doi:10.1080/0142159X.2018.1497149

McKail, R., Hodge, S., Daiches, A., & Misca, G. (2017). Life stories of international Romanian adoptees: A narrative study. *Adoption Quarterly*, *20*(4), 309–328. doi:10.1080/10926755.2017.1349700

McKenna, B., Myers, M. D., & Newman, M. (2017). Social media in qualitative research: Challenges and recommendations. *Information and Organization*, *27*(2), 87–99. doi:10.1016/j.infoandorg.2017.03.001

McKenna, L., & Gray, R. (2018). The importance of ethics in research publications. *Collegian*, *25*(2), 147–148. doi:10.1016/j.colegn.2018.02.006

McLean, K. A., Hardie, S., Paul, A., Paul, G., Savage, I., Shields, P., … Harden, J. (2017). Knowledge and attitudes towards disability in Moldova: A qualitative study of young people's views. *Disability and Health Journal*, *10*(4), 632–635.

doi:10.1016/j.dhjo.2017.01.004

Meinert, E., Van Velthoven, M., Brindley, D., Alturkistani, A., Foley, K., Rees, S., . . . de Pennington, N. (2018). The Internet of things in health care in Oxford: Protocol for proof-of-concept projects. *JMIR Research Protocols*, *7*(12), 1–12. doi:10.2196/12077

Meintjes, K. F., & Nolte, A. G. W. (2015). Parents' experience of childhood atopic eczema in the public health sector of Gauteng. *Curationis*, *38*(1). doi:10.4102/curationis.v38i1.121

Memon, M. S., Shaikh, S. A., Shaikh, A. R., Fahim, M. F., Mumtaz, S. N., & Ahmed, N. (2014). An assessment of knowledge, attitude and practices (KAP) towards diabetes and diabetic retinopathy in a suburban town of Karachi. *Pakistan Journal of Medical Sciences*, *31*(1), 183–188. doi:10.12669/pjms.311.6317

Menard, P., Warkentin, M., & Lowry, P. B. (2018). The impact of collectivism and psychological ownership on protection motivation: A cross-cultural examination. *Computers & Security*, *75*, 147–166. doi:10.1016/j.cose.2018.01.020

Mercer-Mapstone, L., Rifkin, W., Louis, W., & Moffat, K. (2017). Meaningful dialogue outcomes contribute to laying a foundation for social licence to operate. *Resources Policy*, *53*, 347–355. doi:10.1016/j.resourpol.2017.07.004

Miranda, M. J. A. (2018). Enhancing cybersecurity awareness training: A comprehensive phishing exercise approach. *International Management Review*, *14*(2), 5–10. Retrieved from http://www.imrjournal.org

Misenheimer, K. J. (2016). Faculty, staff, and student responsibilities for computer and

information security on campus. *Journal of Information Systems Technology and Planning*, *8*(19), 1–11. Retrieved from http://www.intellectbase.org/journals.php#JISTP

Mohurle, S., & Patil, M. (2017). A brief study of Wannacry threat: Ransomware attack 2017. *International Journal of Advanced Research in Computer Science*, *8*(5), 1938–1940. doi:10.26483/ijarcs.v8i5.4021

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly*, *42*(1), 285–311. doi:10.25300/MISQ/2018/13853

Moore, A. J., Blom, A. W., Whitehouse, M. R., & Gooberman-Hill, R. (2017). Managing uncertainty - a qualitative study of surgeons' decision-making for one-stage and two-stage revision surgery for prosthetic hip joint infection. *BMC Musculoskeletal Disorders*, *18*(1). doi:10.1186/s12891-017-1499-z

Morse, J. M. (2016). Underlying ethnography. *Qualitative Health Research*, *26*(7), 875–876. doi:10.1177/1049732316645320

Mourtada, R., Schlecht, J., & DeJong, J. (2017). A qualitative study exploring child marriage practices among Syrian conflict-affected populations in Lebanon. *Conflict and Health*, *11*(S1). doi:10.1186/s13031-017-0131-z

Murdoch-Flowers, J., Tremblay, M.-C., Hovey, R., Delormier, T., Gray-Donald, K., Delaronde, E., & Macaulay, A. C. (2017). Understanding how Indigenous culturally-based interventions can improve participants' health in Canada. *Health Promotion International*. doi:10.1093/heapro/dax059

Murray, A., Luo, T., & Franklin, T. (2019). Embracing a technologically enhanced environment: Teachers' experience educating students in an always-on and connected bring your own device (BYOD) classroom. *International Journal on E-Learning*, *18*(1), 53–78. Retrieved from http://www.aace.org/pubs/ijel

Myers, S. E., & Downs, R. A. (1968). Comparative findings in school systems with differing approaches to dental health education. *Journal of School Health*, *38*(9), 604–611. doi:10.1111/j.1746-1561.1968.tb04284.x

Myers, S. P., Hill, K. A., Nicholson, K. J., Neal, M. D., Hamm, M. E., Switzer, G. E., … Littleton, E. B. (2018). A qualitative study of gender differences in the experiences of general surgery trainees. *Journal of Surgical Research*, *228*, 127–134. doi:10.1016/j.jss.2018.02.043

Najjar, D., & Fares, P. (2017). Managerial motivational practices and motivational differences between blue- and white-collar employees: Application of Maslow's theory. *International Journal of Innovation, Management and Technology*, *8*(2), 81–84. doi:10.18178/ijimt.2017.8.2.707

National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. (1978). *The Belmont report: Ethical principles and guidelines for the protection of human subjects of research* (No. DHEW-OS-78-0012). Bethesda, MD. Retrieved from https://files.eric.ed.gov/fulltext/ED183582.pdf

Nilsen, M., & Størkersen, K. V. (2018). Permitted to be powerful? A comparison of the possibilities to regulate safety in the Norwegian petroleum and maritime

industries. *Marine Policy*, *92*, 30–39. doi:10.1016/j.marpol.2018.01.014

Niroomand, M., Ghasemi, S. N., Karimi-Sari, H., Kazempour-Ardebili, S., Amiri, P., & Khosravi, M. H. (2016). Diabetes knowledge, attitude and practice (KAP) study among Iranian in-patients with type-2 diabetes: A cross-sectional study. *Diabetes & Metabolic Syndrome: Clinical Research & Reviews*, *10*(1), S114–S119. doi:10.1016/j.dsx.2015.10.006

Njaramba, J., Whitehouse, H., & Lee-Ross, D. (2018). Approach towards female African migrant entrepreneurship research. *Entrepreneurship and Sustainability Issues*, *5*(4), 1043–1053. doi:10.9770/jesi.2018.5.4(24)

Ogie, R. (2016). Bring your own device: An overview of risk assessment. *IEEE Consumer Electronics Magazine*, *5*(1), 114–119. doi:10.1109/MCE.2015.2484858

Oguz Hacat, S. (2018). Assessment of the basic law lesson consistent with the opinions of social studies pre-service teachers. *International Journal of Higher Education*, *7*(1), 103–110. doi:10.5430/ijhe.v7n1p103

Oluwatimi, O., Midi, D., & Bertino, E. (2017). Overview of mobile containerization approaches and open research directions. *IEEE Security & Privacy*, *15*(1), 22–31. doi:10.1109/MSP.2017.12

Origlia Ikhilor, P., Hasenberg, G., Kurth, E., Stocker Kalberer, B., Cignacco, E., & Pehlke-Milde, J. (2018). Barrier-free communication in maternity care of allophone migrants: BRIDGE study protocol. *Journal of Advanced Nursing*, *74*(2), 472–481. doi:10.1111/jan.13441

Panagiotis, G. (2017). A qualitative analysis of the global IFRS adoption. Trustees perspective. *Human and Social Studies*, *6*(2), 59–70. doi:10.1515/hssr-2017-0014

Percy, W. H., Kostere, K., & Kostere, S. (2015). Generic qualitative research in psychology. *The Qualitative Report*, *20*(2), 76–85. Retrieved from http://nsuworks.nova.edu/tqr/

Perry, J., Johnson, I., Popat, H., Morgan, M. Z., & Gill, P. (2018). Adolescent perceptions of orthodontic treatment risks and risk information: A qualitative study. *Journal of Dentistry*, *74*, 61–70. doi:10.1016/j.jdent.2018.04.011

Phillips, M., & Lu, J. (2018). A quick look at NVivo. *Journal of Electronic Resources Librarianship*, *30*(2), 104–106. doi:10.1080/1941126X.2018.1465535

Pinchot, J., & Paullet, K. (2015). Bring your own device to work: Benefits, security risks, and governance issues. *Issues in Information Systems*, *16*(3). Retrieved from http://www.iacis.org/iis/iis.php

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems*, *32*(4), 179–214. doi:10.1080/07421222.2015.1138374

Pretto, A. (2017). Methodological reflections on the study of disability. *Espacio Abierto*, *26*(3), 47–66. Retrieved from https://dialnet.unirioja.es/revistas/editor/4098

Raghunath, R., Anker, C., & Nortcliffe, A. (2018). Are academics ready for smart learning? *British Journal of Educational Technology*, *49*(1), 182–197. doi:10.1111/bjet.12532

Raisinghani, M. S. (2016). An interview with Dennis Hoebee. *Journal of Information Technology Case and Application Research*, *18*(2), 120–123. doi:10.1080/15228053.2016.1197019

Ranney, M. L., Meisel, Z. F., Choo, E. K., Garro, A. C., Sasson, C., & Morrow Guthrie, K. (2015). Interview-based qualitative research in emergency care part II: Data collection, analysis and results Reporting. *Academic Emergency Medicine*, *22*(9), 1103–1112. doi:10.1111/acem.12735

Raymond, C., Profetto-McGrath, J., Myrick, F., & Strean, W. B. (2018). Balancing the seen and unseen: Nurse educator as role model for critical thinking. *Nurse Education in Practice*, *31*, 41–47. doi:10.1016/j.nepr.2018.04.010

Razak, N. A., Marmaya, N. H., & Karim, R. A. (2018). Adaptive behavior towards work environment among internship students. *International Journal of Academic Research in Business and Social Sciences*, *8*(11), 130–137. doi:10.6007/IJARBSS/v8-i11/4889

Razzaghi, M. R., & Afshar, L. (2016). A conceptual model of physician-patient relationships: a qualitative study. *Journal of Medical Ethics & History of Medicine*, *9*(14). Retrieved from http://ijme.tums.ac.ir/

Roache, B., & Kelly, J. (2018). A research method to explore midwives' views of national maternity service reforms. *Women and Birth*, *31*(3), e216–e221. doi:10.1016/j.wombi.2017.09.014

Rocha Flores, W., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness.

Computers & Security, *59*, 26–44. doi:10.1016/j.cose.2016.01.004

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, *91*(1), 93–114. doi:10.1080/00223980.1975.9915803

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo & R. E. Petty (Eds.), *Social psychophysiology: A sourcebook* (pp. 153–176). New York: Guilford Press.

Ronchi, F., Lewis, L., Hauck, Y. L., & Doherty, D. A. (2018). Exploring young pregnant smokers' experiences with a self-nominated non-smoking buddy. *Midwifery*, *59*, 68–73. doi:10.1016/j.midw.2018.01.002

Rosenfeld, E., Kinney, S., Weiner, C., Newall, F., Williams, A., Cranswick, N., … Manias, E. (2018). Interdisciplinary medication decision making by pharmacists in pediatric hospital settings: An ethnographic study. *Research in Social and Administrative Pharmacy*, *14*(3), 269–278. doi:10.1016/j.sapharm.2017.03.051

Ross, M. W., Iguchi, M. Y., & Panicker, S. (2018). Ethical aspects of data sharing and research participant protections. *American Psychologist*, *73*(2), 138–145. doi:10.1037/amp0000240

Ruthven, J. S. (2017). Affect and the "really real": The politics of HIV/AIDS framing in South African theater. *Medical Anthropology*, *36*(8), 729–743. doi:10.1080/01459740.2017.1353979

Ruwhiu, D., Amoamo, M., Ruckstuhl, K., Kapa, J., & Eketone, A. (2018). Success factors of Māori entrepreneurs: A regional perspective. *Journal of Management &*

Organization, 1–21. doi:10.1017/jmo.2018.45

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*(Supplement C), 65–78. doi:10.1016/j.cose.2015.05.012

Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior*, *57*, 442–451. doi:10.1016/j.chb.2015.12.037

Safar, A. H. (2018). BYOD in higher education: A case study of Kuwait University. *Journal of Educators Online*, *15*(2). doi:10.9743/jeo.2018.15.2.9

Sambo, M., Lembo, T., Cleaveland, S., Ferguson, H. M., Sikana, L., Simon, C., … Hampson, K. (2014). Knowledge, attitudes and practices (KAP) about rabies prevention and control: A community survey in Tanzaniaa. *PLoS Neglected Tropical Diseases*, *8*(12), e3310–e3320. doi:10.1371/journal.pntd.0003310

Sanderson, S. C., Linderman, M. D., Suckiel, S. A., Zinberg, R., Wasserstein, M., Kasarskis, A., … Schadt, E. E. (2017). Psychological and behavioural impact of returning personal results from whole-genome sequencing: the HealthSeq project. *European Journal of Human Genetics*, *25*(3), 280–292. doi:10.1038/ejhg.2016.178

Sarkar, S., Osiyevskyy, O., & Clegg, S. R. (2018). Incumbent capability enhancement in response to radical innovations. *European Management Journal*, *36*(3), 353–365. doi:10.1016/j.emj.2017.05.006

Satalkar, P., Elger, B. S., & Shaw, D. M. (2016). Stakeholder views on participant

selection for first-in-human trials in cancer nanomedicine. *Current Oncology*, *23*(6), 530. doi:10.3747/co.23.3214

Scheel-Sailer, A., Post, M. W., Michel, F., Weidmann-Hügle, T., & Baumann Hölzle, R. (2017). Patients' views on their decision making during inpatient rehabilitation after newly acquired spinal cord injury-A qualitative interview-based study. *Health Expectations*, *20*(5), 1133–1142. doi:10.1111/hex.12559

Schoonenboom, J., & Johnson, R. B. (2017). How to construct a mixed methods research design. *Kölner Zeitschrift Für Soziologie Und Sozialpsychologie*, *69*(Suppl. 2), 107–131. doi:10.1007/s11577-017-0454-1

Schröder, S., Soliman, M., & Riebisch, M. (2018). Architecture enforcement concerns and activities - An expert study. *Journal of Systems and Software*, *145*, 79–97. doi:10.1016/j.jss.2018.08.025

Sebescen, N., & Vitak, J. (2017). Securing the human: Employee security vulnerability risk in organizational settings. *Journal of the Association for Information Science and Technology*, *68*(9), 2237–2247. doi:10.1002/asi.23851

Sepasgozar, S. M. E., Davis, S., Loosemore, M., & Bernold, L. (2017). An investigation of modern building equipment technology adoption in the Australian construction industry. *Engineering, Construction and Architectural Management*, *25*(8), 1203–1221. doi:10.1108/ECAM-06-2016-0149

Shah, M. A. R., Husnain, M., & Zubairshah, A. (2018). Factors affecting brand switching behavior in telecommunication industry of Pakistan: A qualitative investigation. *American Journal of Industrial and Business Management*, *08*(02), 359–372.

doi:10.4236/ajibm.2018.82022

Shahri, A. B., Ismail, Z., & Mohanna, S. (2016). The impact of the security competency on "self-efficacy in information security" for effective health information security in Iran. *Journal of Medical Systems*, *40*(11), 241–249. doi:10.1007/s10916-016-0591-5

Shillair, R., Cotten, S. R., Tsai, H.-Y. S., Alhabash, S., LaRose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior*, *48*(Supplement C), 199–207. doi:10.1016/j.chb.2015.01.046

Siew, C. T., Mazzucchelli, T. G., Rooney, R., & Girdler, S. (2017). A specialist peer mentoring program for university students on the autism spectrum: A pilot study. *PLoS One*, *12*(7). doi:10.1371/journal.pone.0180854

Sil, A., & Das, N. K. (2017). Informed consent process: Foundation of the researcher–participant bond. *Indian Journal of Dermatology*, *62*(4), 380–386. doi:10.4103/ijd.IJD_272_17

Simonson, M. (2016). Assumptions and distance education. *Distance Learning*, *13*(1), 60–59.

Singh, G., Pasricha, S., Nanda, G. S., Singh, H., Bandyopadhyay, K., & Ray, G. (2018). Internet use behavior, risk profile and 'problematic internet use' among undergraduate medical students: An epidemiological study. *International Journal of Community Medicine and Public Health*, *5*(2), 532. doi:10.18203/2394-6040.ijcmph20180115

Singh, M. M., Chan, C. W., & Zulkefli, Z. (2017). Security and privacy risks awareness for bring your own device (BYOD) paradigm. *International Journal of Advanced Computer Science and Applications*, *8*(2), 53–62. doi:10.14569/IJACSA.2017.080208

Singhal, D. K., Acharya, S., & Thakur, A. S. (2017). Maternal knowledge, attitude and practices regarding oral health of preschool children in Udupi taluk, Karnataka, India. *Journal of International Dental & Medical Research*, *10*(2), 270–277. Retrieved from http://www.ektodermaldisplazi.com/journal.htm

Skiba, D. J. (2016). On the horizon: Trends, challenges, and educational technologies in higher education. *Nursing Education Perspectives*, *37*(3), 183–185. doi:10.1097/01.NEP.0000000000000019

Smith, B., & McGannon, K. R. (2018). Developing rigor in qualitative research: problems and opportunities within sport and exercise psychology. *International Review of Sport and Exercise Psychology*, *11*(1), 101–121. doi:10.1080/1750984X.2017.1317357

Smith, W. P. (2017). "Can we borrow your phone? Employee privacy in the BYOD era." *Journal of Information, Communication and Ethics in Society*, *15*(4), 397–411. doi:10.1108/JICES-09-2015-0027

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). A meta-analysis of studies on protection motivation theory and information security behaviour. *International Journal of Information Security and Privacy*, *9*(1), 26–46. doi:10.4018/IJISP.2015010102

Song, Y. (2016). “We found the ‘black spots’ on campus on our own”: development of inquiry skills in primary science learning with BYOD (bring your own device). *Interactive Learning Environments*, *24*(2), 291–305. doi:10.1080/10494820.2015.1113707

Song, Y., & Kong, S. C. (2017). Affordances and constraints of BYOD (bring your own device) for learning and teaching in higher education: Teachers’ perspectives. *The Internet and Higher Education*, *32*, 39–46. doi:10.1016/j.iheduc.2016.08.004

Spangler, S. C., Rodi, A., & Kiernan, M. (2016). Case study: BYOD in the higher education classroom: Distraction or disruption? The adoption of Spangler’s 2016 digital human IT integration charting system. *Issues in Information Systems*, *17*(3). Retrieved from http://www.iacis.org/iis/iis.php

Spronken-Smith, R., Buissink-Smith, N., Bond, C., & Grigg, G. (2015). Graduates’ orientations to higher education and their retrospective experiences of teaching and learning. *Teaching & Learning Inquiry*, *3*(2), 55–70. doi:10.20343/teachlearninqu.3.2.55

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, *92*, 178–188. doi:10.1016/j.future.2018.09.063

State of Play Report BYOD, CYOD, BYOT, BYOA, and More. (2014). *ITNOW*, *56*(3), 56–57. doi:10.1093/itnow/bwu083

Stellefson, M., Paige, S. R., Alber, J. M., Barry, A. E., & James, D. (2015). Proposing ethical practice standards for community-engaged research in health education.

American Journal of Health Education, *46*(2), 61–66. doi:10.1080/19325037.2014.997942

Stevenson, M. E., & Hedberg, J. G. (2017). Mobilizing learning: A thematic review of apps in K-12 and higher education. *Interactive Technology and Smart Education*, *14*(2), 126–137. doi:10.1108/ITSE-02-2017-0017

Sun, F.-K., Long, A., Tseng, Y. S., Huang, H.-M., You, J.-H., & Chiang, C.-Y. (2016). Undergraduate student nurses' lived experiences of anxiety during their first clinical practicum: A phenomenological study. *Nurse Education Today*, *37*, 21–26. doi:10.1016/j.nedt.2015.11.001

Swanson, E. (2017). Why the nipple is an unreliable marker for measuring breast ptosis. *Aesthetic Surgery Journal*, *37*(2), NP24–NP26. doi:10.1093/asj/sjw195

Tang, C. J., Zhou, W. T., Chan, S. W.-C., & Liaw, S. Y. (2018). Interprofessional collaboration between junior doctors and nurses in the general ward setting: A qualitative exploratory study. *Journal of Nursing Management*, *26*(1), 11–18. doi:10.1111/jonm.12503

Tchao, E. T., Ansah, R. Y., & Kotey, S. D. (2017). Barrier free internet access: Evaluating the cyber security risk posed by the adoption of bring your own devices to e-learning network infrastructure. *International Journal of Computer Applications*, *176*(3), 53–62. doi:10.5120/ijca2017915581

Tenório, A., Loos, T., & Tenório, T. (2017). Perceptions of tutors and students on affectivity and conflict mediation in an e learning course for the Brazilian police. *Revista Iberoamericana de Educación a Distancia*, *20*(1), 223–240.

doi:10.5944/ried.20.1.15806

Teusner, A. (2016). Insider research, validity issues, and the OHS professional: one person's journey. *International Journal of Social Research Methodology*, *19*(1), 85–96. doi:10.1080/13645579.2015.1019263

Theobald, K. A., & Ramsbotham, J. (2019). Inquiry-based learning and clinical reasoning scaffolds: An action research project to support undergraduate students' learning to 'think like a nurse.' *Nurse Education in Practice*, *38*, 59–65. doi:10.1016/j.nepr.2019.05.018

Thomas, D. R. (2017). Feedback from research participants: are member checks useful in qualitative research? *Qualitative Research in Psychology*, *14*(1), 23–41. doi:10.1080/14780887.2016.1219435

Thompson, N., McGill, T. J., & Wang, X. (2017). "Security begins at home": Determinants of home computer and mobile device security behavior. *Computers & Security*, *70*, 376–391. doi:10.1016/j.cose.2017.07.003

Tinmaz, H., & Lee, J. H. (2019). A perceptional analysis of BYOD (bring your own device) for educational or workplace implementations in a South Korean case. *Participatory Educational Research*, *6*(2), 51–64. doi:10.17275/per.19.12.6.2

Toperesu, B.-A., & Van, B. J.-P. (2017). Organisational capabilities required for enabling employee mobility through bring-your-own-device concept. *Business Systems Research Journal*, *8*(1), 17–29. doi:10.1515/bsrj-2017-0002

Tsai, H. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory

perspective. *Computers & Security*, *59*(Supplement C), 138–150. doi:10.1016/j.cose.2016.02.009

University of California. (2019). *BFB-IS-3: Electronic Information Security*. Retrieved from https://policy.ucop.edu/doc/7000543/BFB-IS-3

Urban, A., & Schweda, M. (2018). Clinical and personal utility of genomic high-throughput technologies: perspectives of medical professionals and affected persons. *New Genetics and Society*, *37*(2), 153–173. doi:10.1080/14636778.2018.1469976

Utter, C. J., & Rea, A. (2015). The "bring your own device" conundrum for organizations and investigators: An examination of the policy and legal concerns in light of investigatory challenges. *Digital Forensics, Security and Law. Journal*, *10*(2), 55–71. doi:10.15394/jdfsl.2015.1202

VanLeeuwen, C., & Torondel, B. (2018). Exploring menstrual practices and potential acceptability of reusable menstrual underwear among a Middle Eastern population living in a refugee setting. *International Journal of Women's Health*, *10*, 349–360. doi:10.2147/IJWH.S152483

van Rijnsoever, F. J. (2017). (I can't get no) saturation: A simulation and guidelines for sample sizes in qualitative research. *PLoS One*, *12*(7), e0181689–e081705. doi:10.1371/journal. pone.0181689

Verkijika, S. F. (2018). Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret. *Computers & Security*, *77*, 860–870. doi:10.1016/j.cose.2018.03.008

Villarreal Larrinaga, O. (2017). Is it desirable, necessary and possible to perform research using case studies? *Cuadernos de Gestion*, *17*(1), 147–171. doi:10.5295/cdg.140516ov

Vorakulpipat, C., Sirapaisan, S., Rattanalerdnusorn, E., & Savangsuk, V. (2017). A policy-based framework for preserving confidentiality in BYOD environments: A review of information security perspectives. *Security and Communication Networks*, *2017*. doi:10.1155/2017/2057260

Vosper, H., & Hignett, S. (2018). A UK perspective on human factors and patient safety education in pharmacy curricula. *American Journal of Pharmaceutical Education*, *82*(3), 227–239. doi:10.5688/ajpe6184

Wang, J., Liu-Lastres, B., Ritchie, B. W., & Mills, D. J. (2019). Travellers' self-protections against health risks: An application of the full protection motivation theory. *Annals of Tourism Research*, *78*, 1–12. doi:10.1016/j.annals.2019.102743

Wanja, I. (2018). Developing a threat matrix for smart devices in a university network towards a secure local area network ecosystem. *Mara Research Journal of Computer Science & Information Security*, *3*(1), 1–11. Retrieved from http://compsc.mrjournals.org/index.php/MRJCSIS/index

Warburton, J., Moore, M., & Oppenheimer, M. (2017). Challenges to the recruitment and retention of volunteers in traditional nonprofit organizations: A case study of Australian meals on wheels. *International Journal of Public Administration*, 1–13. doi:10.1080/01900692.2017.1390581

Warkentin, M., Johnston, A. C., Shropshire, J., & Barnett, W. D. (2016). Continuance of

protective security behavior: A longitudinal study. *Decision Support Systems*, *92*(Supplement C), 25–35. doi:10.1016/j.dss.2016.09.013

Wendot, S., Scott, R. H., Nafula, I., Theuri, I., Ikiugu, E., & Footman, K. (2018). Evaluating the impact of a quality management intervention on post-abortion contraceptive uptake in private sector clinics in western Kenya: A pre- and post-intervention study. *Reproductive Health*, *15*(1). doi:10.1186/s12978-018-0452-4

Westcott, R., Ronan, K., Bambrick, H., & Taylor, M. (2017). Expanding protection motivation theory: investigating an application to animal owners and emergency responders in bushfire emergencies. *BMC Psychology*, *5*, 13. doi:10.1186/s40359-017-0182-3

Wilson, S. (2018). A framework for security technology cohesion in the era of the GDPR. *Computer Fraud & Security*, *2018*(12), 8–11. doi:10.1016/S1361-3723(18)30119-2

Winkel, A. F., Honart, A. W., Robinson, A., Jones, A.-A., & Squires, A. (2018). Thriving in scrubs: A qualitative study of resident resilience. *Reproductive Health*, *15*(1). doi:10.1186/s12978-018-0489-4

Winters, K., Carvalho, E., & Oliver, T. (2017). The 2015 qualitative election study of Britain. *Research Data Journal for the Humanities and Social Sciences*. doi:10.1163/24523666-01000007

Wirth, A. (2018). All together now. *Biomedical Instrumentation & Technology*, *52*(5), 392–394. doi:10.2345/0899-8205-52.5.392

Woods, T. M., Acosta, W. R., Chung, E. P., Cox, A. G., Garcia, G. A., Klucken, J. R., &

Chisholm-Burns, M. (2016). Academic freedom should be redefined: Point and counterpoint. *American Journal of Pharmaceutical Education*, *80*(9), 1–5. doi:10.5688/ajpe809146

Woodside, J. M., & Amiri, S. (2014). Bring your own technology (BYOT) to education. *Journal of Systemics, Cybernetics and Informatics*, *12*(3), 38–40. Retrieved from http://www.iiisci.org/Journal/SCI/Home.asp

Xerri, D. (2018). The use of interviews and focus groups in teacher research. *The Clearing House: A Journal of Educational Strategies, Issues and Ideas*, *91*(3), 140–146. doi:10.1080/00098655.2018.1436820

Xiao, H., Li, S., Chen, X., Yu, B., Gao, M., Yan, H., & Okafor, C. N. (2014). Protection motivation theory in predicting intention to engage in protective behaviors against schistosomiasis among middle school students in rural China. *PLoS Neglected Tropical Diseases*, *8*(10), e3246. doi:10.1371/journal.pntd.0003246

Yasin, M. M., Czuchry, A. J., & Small, M. H. (2018). Organizational security: A conceptual framework and implementation issues. *Competition Forum*, *16*(1), 38–49. Retrieved from https://link.gale.com

Yilmaz, K. (2013). Comparison of quantitative and qualitative research traditions: Epistemological, theoretical, and methodological differences. *European Journal of Education*, *48*(2), 311–325. doi:10.1111/ejed.12014

Yin, H., Ye, J., Gao, H., Li, Q., Tian, Q., Wang, W., & Di, W. (2017). Knowledge, attitude and practice about reproductive health of perimenopausal and postmenopausal women in Shanghai: a cross-sectional and intervention study.

International Journal of Clinical and Experimental Medicine, *10*(7), 10944–10951. Retrieved from http://www.ijcem.com/

Zahedi, F. M., Abbasi, A., & Chen, Y. (2015). Fake-website detection tools: Identifying elements that promote individuals' use and enhance their performance. *Journal of the Association for Information Systems*, *16*(6), 448–484. doi:10.17705/1jais.00399

Zhou, Z. (2017). Integrated education model of information technology and financial accounting. *Eurasia Journal of Mathematics, Science and Technology Education*, *13*(10), 6767–6777. doi:10.12973/ejmste/78272

Appendix A: Copyright Permission From Taylor and Francis

Copyright Clearance Center RightsLink®

Home | Create Account | Help

Routledge Taylor & Francis Group

Title: A Protection Motivation Theory of Fear Appeals and Attitude Change1
Author: Ronald W. Rogers
Publication: The Journal of Psychology
Publisher: Taylor & Francis
Date: Sep 1, 1975
Rights managed by Taylor & Francis

LOGIN

If you're a copyright.com user, you can login to RightsLink using your copyright.com credentials.

Already **a RightsLink user** or want to learn more?

Thesis/Dissertation Reuse Request

Taylor & Francis is pleased to offer reuses of its content for a thesis or dissertation free of charge contingent on resubmission of permission request if work is published.

BACK CLOSE WINDOW

Appendix B: Copyright Permission From Guilford Press

Re: Permission request

Angela Whalen <Angela.Whalen@guilford.com> on behalf of
GP Permissions <Permissions@guilford.com>

Mon 6/11/2018 8:21 AM

To:Hai Nguyen <hai.nguyen@waldenu.edu>;

One-time non-exclusive world rights in the English language for print and electronic formats are granted for your requested use of the selections below in your dissertation to be published by Walden University.

Permission fee due: No Charge

This permission is subject to the following conditions:

1. A credit line will be prominently placed and include: the author(s), title of book, editor, copyright holder, year of publication and "Reprinted with permission of Guilford Press" (or author's name where indicated).

2. Permission is granted for one-time use only as specified in your request. Rights herein do not apply to future editions, revisions or other derivative works. Should you wish to reproduce this material in future revisions and editions of your work, permission will need to be re-secured from Guilford. Certain fees may apply at that time.

3. The requestor agrees to secure written permission from the original author where indicated.

4. The permission granted herein does not apply to quotations from other sources that have been incorporated in the Selection.

5. The requestor warrants that the material shall not be used in any manner which may be considered derogatory to this title, content, or authors of the material or to Guilford Press.

6. Guilford retains all rights not specifically granted in this letter.

Best wishes,
Angela Whalen
Rights & Permissions

Guilford Publications, Inc.
370 Seventh Avenue, Suite 1200
New York, NY 10001-1020

permissions@guilford.com
http://www.guilford.com/permissions

From: "Hai Nguyen" <hai.nguyen@waldenu.edu>
To: "permissions@guilford.com" <permissions@guilford.com>
Cc: "Hai Nguyen" <hai.nguyen@waldenu.edu>
Date: 06/07/2018 02:20 AM
Subject: Permission request

Dear Guilford Press:

I am completing a doctoral dissertation at Walden University entitled "Strategies to Secure an Environment to Support BYOD in a University Setting." I would like your permission to reproduce in my dissertation, figures from:

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo & R. E. Petty (Eds.), *Social psychophysiology: A sourcebook* (pp. 153–176). New York: Guilford Press.

The figure to be reproduced is *Figure 6-2. Schema of protection motivation theory* on page 168.

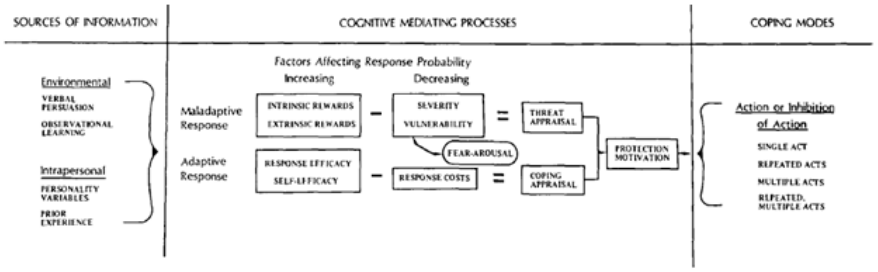

FIGURE 6-2. Schema of protection motivation theory.

The requested permission extends to any future revisions and editions of my dissertation, including non-exclusive world rights in all languages, and to the prospective publication of my dissertation by ProQuest through its ProQuest® Dissertation Publishing business. ProQuest may produce and sell copies of my dissertation on demand and may make my dissertation available for free internet download at my request. These rights will in no way restrict republication of the material in any other form by you or by others authorized by you. Your approval will also confirm that you own [or your company owns] the copyright to the above described material.

If these arrangements meet with your approval, please reply to this email with your decision. Thank you very much.

Sincerely,

Hai Nguyen
Candidate, DIT
Walden University
hai.nguyen@waldenu.edu

Appendix C: Interview Protocol

Interview Protocol

Preinterview

Contact the participant to schedule the interview. The participant will determine the location and time that is most convenient for the participant. The preferred interview location will be a place that provides security and privacy.

Meet the participant at the agreed upon interview location and time.

Provide an overview and purpose of the study.

Let the participant know how the interview data will be used.

Inform the participant that complete anonymity is not possible due to the interviewing and informed consent process; however, the participant's identity will only be known to me, the researcher.

Indicate the measures that will be taken to protect the participant's confidentiality, both directly and indirectly.

Inform the participant that the session will be recorded and that notes will be taken.

Obtain consent.

Main research question: What strategies do IT security professionals working in a university setting use to secure an environment to support BYOD in a university system?

Interview

1. Please tell me about… (*background*)
    a. Yourself.
    b. Your experience in network security.
        i. How long?
2. How many users do you support?
3. What does security mean to you?
4. What are some of the factors that influenced the adoption of BYOD in your organization? (*PMT – Sources of information)*
5. What types of BYOD are allowed on your network? (*PMT – Sources of information)*
    a. Roughly about how many BYOD devices are on your network at any time?
6. What strategies have you used to secure an environment to support BYOD? (*PMT – Coping appraisal, PMT – Coping modes)*
7. How would you determine which strategies are implemented? (*PMT – Coping appraisal)*
8. What type of information is accessible via personal devices? (*PMT – Threat appraisal)*
9. What is involved when managing a network where BYOD is present? (*PMT – Sources of information)*
10. How would you describe your role and involvement in the acquisition and implementation of the security strategies? (*PMT – Coping appraisal)*
11. How would you determine whether the strategies you have implemented are effective? (*PMT – Threat appraisal)*
12. How comfortable are you with your current security strategy regarding BYOD? (*Strategies, PMT – Coping appraisal)*

a. Is there anything you would change? *(PMT – Coping modes)*

Postinterview

Remind participant that participation is voluntary.

Provide contact information in case participant decides to withdraw from the study.

Assure participant that their identity will be de-identified.

Provide the participant with a summary of the study findings to allow the participant the opportunity to stay or withdraw from the study. Inform the participant that a copy of the completed manuscript will be provided once published.

Inform participant that data will be secured for 5 years then destroyed.