2020

IT Security Managers' Strategies for Mitigating Data Breaches in Texas School Districts

Mercy Ikhuoria Nwankwo
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Mercy Nwankwo

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. Bob Duhainy, Committee Chairperson, Information Technology Faculty
Dr. Steven Case, Committee Member, Information Technology Faculty
Dr. Jodine Burchell, University Reviewer, Information Technology Faculty

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

Walden University
2020

Abstract

IT Security Managers' Strategies for Mitigating Data Breaches in Texas School Districts

by

Mercy Ikhuoria Nwankwo

MS, Walden University, 2017

MIT, University of Lagos, 2010

BS, University of Benin, 2004

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

November 2020

Abstract

School districts are increasingly becoming a prime target for cybercriminals. As a result, information technology (IT) security managers in Texas school districts are concerned about hackers gaining access to network resources that could lead to data breaches on their network. Grounded in the technology threat avoidance theory, the purpose of this qualitative multiple case study was to explore strategies IT security managers use to mitigate data breaches in school district networks in Texas. The participants comprised 6 IT security managers in 3 Texas school districts whose roles involved managing and implementing data security strategies. Data collection involved conducting semistructured interviews (*n* = 6) and reviewing organizational, technical, district, and public documents (*n* = 12). Methodological triangulation was suitable for analyzing the emerging themes, and a follow-up member check served to increase data validity. Four major themes emerged: data security breach frequency and risk, data breach safe practices and control attempts, prevention challenges and response setbacks, and recommendations for strengthening data security prevention. Recommendations are for IT security managers to implement multiple security layers, promote mandatory user training, improve existing security policies, and encourage the buy-in by district leadership to support operational, technical, administrative, and physical security control synergy. The implications for positive social change include potential guidance for institutional decision-makers and IT security managers to protect their resources, promote digital transformation, comply with regulatory mandates, and generate user trust and loyalty.

IT Security Managers' Strategies for Mitigating Data Breaches in Texas School Districts

by

Mercy Ikhuoria Nwankwo

MS, Walden University, 2017

MIT, University of Lagos, 2010

BS, University of Benin, 2004

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

November 2020

Dedication

I dedicate this entire work to my late parents, who worked so hard to see me get educated, but never saw me accomplish my bachelors' degree and wear that fulfilled convocation regalia. Their love for education, hard work, perseverance, and determination craved a path for me to succeed today. Mom, you first taught me how to read aloud at age three, even when you didn't have a fair chance of getting a higher education you painstakingly sought for, owing to gender discrimination and unequal opportunities for women towards education in your days. You taught me to work hard in life and to get gritter with life's endeavor. To all women everywhere, old, or young facing one form of discrimination or another, this degree is dedicated to you.

Acknowledgments

I thank the good Lord for the gift of life, overflowing love, guidance, protection, and the many other blessings, including the grace to complete this study.

My appreciation goes to my advisors and committee members: Dr. Bob Duhainy, Dr. Steven Case, Dr. J. Burchell, and Dr. Gail Miles, for their mentorship, guidance, leadership, and direction during this research. A special thanks to my chair, Dr. Bob Duhainy, for opening an excellent pathway for me to succeed and complete my DIT program. I highly appreciate the many times you made calls and responded to my many e-mail messages to ensure I am on track with my study and provide a more precise roadmap for me. If not for your active engagement and mentorship, I doubt if I would have completed this DIT program successfully. Special thanks to Dr. Steven Case for your continued motivation and reassurance. I want to appreciate Dr. Burchell for putting in so much effort and time to go through my entire project to align with Walden Doctoral studies' goals and objectives. A special thanks to Dr. Gail Miles, for her leadership and support. A big thank you goes to all my study participants. I am hopeful you find the results of your effort worthy of your time investment and to my classmates thank you for your continued support and wisdom over these past years.

Finally, I would like to thank my family for putting up with my late nights, lost family weekends, and countless hours of being online researching for this project. Without your love and support, completing this study would not have been possible. I am immensely grateful to my loving husband and daughters, whose strength, prayers, and love I relied on during the cause of this dissertation.

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

The focus of this study was exploring the strategies used by information technology (IT) security managers to mitigate data breaches on their school's network using a qualitative multiple case method. The findings from this study could benefit IT security practice by increasing IT security practitioners' understanding and knowledge of the multifaceted structure of cyber-attacks and data breaches that may lead to more secure school networks an bring about changes that could protect institution information systems from theft and damage attempts. The findings from this study may help IT security professionals and district leaders who have the responsibility to manage a school network to apply a more secure and nonthreatening online experience for students. The study also includes insights that may help identify potential security threats and responses before an incident escalates, may lead to the development of technology designed to keep students safe online, and may provide families an increased assurance of online safety at school.

Background of the Problem

The importance of technology in delivering knowledge in schools is without question. School district administrators apply technology in learning more than at any time in the past (Machado & Chung, 2015). Technology has also made learning and record-keeping easier in the education system (McKnight et al., 2016). However, cybersecurity threats pose significant concerns for many school districts (Selwyn & Bulfin, 2016). Information technology security managers face significant challenges in providing security and protection of sensitive data and personally identifiable information from cyber threat attempts (Soomro, Shah, & Ahmed, 2016). The incentive for attacks by malicious agents is the fact that school networks and technology systems have become repositories for sensitive records of students, staff, and institutions. Malicious agents understand that the potential exists to expose confidential documents and weak applications as technology users transmit data over the internet (Cheng, Liu, & Yao, 2017). Understanding the security threats to school networks and the strategies deployed by IT security managers to mitigate these threats was the primary focus of this study.

Problem Statement

Cybersecurity threats pose significant concerns for many school districts whose employees deploy technology for learning (Selwyn & Bulfin, 2016). In 2015, the educational sector accounted for 7.4% of total cybersecurity breaches, while in 2016 over 360,000 records were potentially at risk of cybersecurity threats, outpacing the banking sector and the government in terms of the total number of data breaches that occurred in the first half of that year (Demers, Harrington, Cianci, & Green, 2017). The general IT problem is that schools' network resources accessed by students for learning that do not have appropriate security measures could be vulnerable to cyber threats. The specific IT problem is that some IT security managers lack the strategies necessary to mitigate data breaches on their school's network.

Purpose Statement

The purpose of this qualitative multiple case study was to explore the strategies used by IT security managers to mitigate data breaches on their school's network. The research population was IT security managers from three school districts in Texas, which is in the south-central region of the United States, with experience executing IT security strategies that protect school networks from a data breach. The findings from this study may benefit information security practice by increasing IT security practitioners' understanding and knowledge of the multifaceted structure of cyber-attacks that may lead to more secure school networks. The implication for positive social change lies in the potential to provide a more secure and nonthreatening online experience for students and possibly offer their parents and families an increased assurance of their wards' online safety while in school.

Nature of the Study

The research methods commonly used in research are qualitative, quantitative, and mixed (McCusker & Gunaydin, 2015). Qualitative researchers use the qualitative approach to gain a deeper understanding of a phenomenon through open dialogue with participants (Hesse-Biber, 2016). I selected the qualitative method to discover the in-depth meaning of an event through interaction with data collected from participants experiences. Researchers use the qualitative research method to address what, how, and why questions to identify and understand the issues raised in studies (Onwuegbuzie & Byers, 2014). Thus, the qualitative method was suitable for this study because the method helps to discover more about the subject through a detailed contextual analysis of numerous activities and their relationships to understanding best security strategies. A quantitative scientist shapes theory through experiments and through the operationalization and manipulation of observed variables, forecasts, correlation, and testing of collated data (Ko, Latoza, & Burnett, 2015). As this study did not involve any experimentation on participants, the quantitative method was not suitable. Mixed-methods research consists of merging both qualitative and quantitative approaches, which involves manipulating variables and testing hypotheses (Antwi & Hamza, 2015; Frels & Onwuegbuzie, 2013; Mayoh & Onwuegbuzie, 2015). I did not conduct mixed-methods research because I explored open-ended inquiries.

The qualitative multiple case study technique was suitable because of its strength in examining existing phenomena without influencing appropriate behaviors. The benefits of conducting a multiple case study are that researchers can analyze data within each situation and across different locations (Gustafsson, 2017). A multiple case study also allows a broader examination of several instrumental bounded cases to develop a more in-depth understanding of the research than a single case can accommodate (Gustafsson, 2017; Mohajan, 2018). Researchers study numerous cases to understand the similarities and differences between facts that can provide that can provide a convincing theory grounded in several empirical evidence (Gustafsson, 2017). Evidence generated from a multiple case study is robust and reliable, and researchers can clarify if the results from findings are invaluable (Mohajan, 2018). Researchers conducting a case study explore, investigate, and describe a real-world event within a bounded, contextual setting (Guetterman, 2015).

Other qualitative designs, such as phenomenology, only seek to gain the truth of the lived experiences of participants in their natural outlook (Giorgi, Giorgi, & Morley, 2017; Murdock, 2018). I did not apply this design, as I did not concentrate on the lived experiences of the participants and thus, they were not relevant to the intent and objectives of this study. Ethnographers combine research design and fieldwork to develop a greater understanding of specific subgroups that scientifically describes the individuals (Bamkin, Maynard, & Goulding, 2016). Ethnography involves an attempt to understand the customs and culture of a group by observing and describing a society from the viewpoint of the subjects of the study (Hammersley, 2018).

I did not rely on or use the strengths of the ethnographic research design because investigating the customs or culture of any social group was not the focus of this study. The narrative approach subsumes a chain of events that can be written or spoken, words, or a visual form, usually from just one or two individuals' lives, to form a cohesive story (Joyce, 2015). The narrative approach generally involves a researcher conducting in-depth interviews, reading documents, and looking for themes to demonstrate how the individual stories illustrate the lives of individuals as told through their own stories (Joyce, 2015). I did not use a narrative design because the focus of this study was not the sequence of events of the life story of an individual's internet use.

Research Question

What strategies do IT security managers use to mitigate data breaches on their school's network?

Interview/Survey Questions

1. What techniques do you use to mitigate data breaches?
2. What strategies do you use to protect and control the flow of data on your network from unauthorized access?
3. How do you manage the challenges faced in implementing these strategies?

4. What kind of technical expertise do IT security managers need to be able to improve data breach prevention within an organization?
5. What kind of setbacks have you encountered when responding to data security breaches?
6. What are some skill sets network security managers lack that are needed to minimize data breaches?
7. How likely will security compliance violations within your organization result in data breaches?
8. How frequently does your organization experience data breaches?
9. What data breach incidents, if any, have you tackled that mainly and negatively impacted your organization?
10. What are some factors that can motivate attackers to target an organization's data?
11. What data security policies and best practices will you suggest that can help mitigate the incidence of data breaches within an organization?
12. How can you reduce the impact or the likelihood of a data breach?
13. What operational IT prevention programs do you have in place that could offer parents and families an increased assurance of their wards' online safety while in school?
14. What recommendations can you provide that may assist IT security managers and leaders in security in implementing proactive data security measures?

Conceptual Framework

The technology threat avoidance theory (TTAT) was the conceptual framework for the study. In 2009, the Liang and Xue developed TTAT using two cognitive methods identified as an appraisal and coping mechanism to determine the individual perception of an IT threat existence and their behavior to avoid the threat (Hewitt, Dolezel, & McLeod, 2017; Liang & Xue, 2010). The theory, therefore, explains individual IT users' behavior of avoiding the threat of malicious information technologies (Liang & Xue, 2009). In 2010, Liang and Xue improved on the theory by testing a technology threat avoidance model to determine the motivation needed to avoid a cyber threat, which is affected positively by the perceived threat (Liang & Xue, 2009; Zahedi, Abbasi, & Chen, 2017). The theory further describes the processes and factors of susceptibility response and self-efficacy that are negatively affected by the cost of response and how IT users engage in threat avoidance behaviors (Hewitt et al., 2017; Liang & Xue, 2010).

The TTAT also recognizes that IT threats occur and that individuals can apply some security techniques with the primary objective of mitigating the threat and its associated cost as much as possible (Zahedi et al., 2017). Das and Khan (2016) used the theory to establish a coping and appraisal framework that enables users to consider the three factors to evaluate when considering the presence of a threat (see Figure 1). The three factors are the extent of redundancy of a security threat if a safeguard measure is applied, the cost of administering the safeguard, and users' expertise in implementing the defense. By leveraging the tenets of this theory, IT security managers may be able to initiate a more efficient institutional IT mechanisms for school networks, provide an IT threat-prevention system that may entail technology deployment and user training, and be able to formulate more effective IT guidelines, practices, and policies.

I selected the TTAT as the conceptual framework for this study because it was suitable for assisting the IT security managers in the Texas school districts under study to determine the current mitigating strategies in place, to explore how to perceive existing threats, and to cope with technology use when faced with a threat. The choice of the TTAT may assist IT security experts to identify operational, technical, and nontechnical procedures such as end-user training, IT security policy, and preventive frameworks to adapt, formulate, and deploy to improve the protection of students and other online users from malicious attacks on the schools' network.

Definition of Terms

Breach: An occurrence in which an individual's name, medical or financial records, or debit card are potentially put at risk either in electronic or paper format (Mozumder, Mahi, Whaiduzzaman, & Mahi, 2017).

Cyber risk: Cyber risk is the operational risks associated with information and technology assets that may result in consequences affecting the confidentiality, availability, or integrity of information or information systems (Biener, Eling, & Wirfs, 2015).

Cybersecurity: The collection of tools, security concepts, security safeguards, policies and guidelines, best practices, risk management approaches, training, actions, assurance, and technologies available to protect cyberspace and organizations' and users' assets (Althonayan & Andronache, 2018).

Data breach: A data breach is an electronically mediated service failure that occurs when sensitive financial, personal, or customer data are released to or accessed by unauthorized parties internal or external to an organization (Goode, Hoehle, Venkatesh, & Brown, 2017).

Data breach severity: The scope, reach, and impact of a firm's data security breach (Martin, Borah, & Palmatier, 2017).

Information security: The process by which digital information assets are protected to ensure confidentiality, integrity, and availability as the main security goals are achieved (Elmrabit, Yang, & Yang, 2015).

Information technology (IT) managers: IT managers are IT personnel experienced in managing IT assets, network infrastructures, technologies, top-level IT roles, and people within an organization or body, including the chief information officers, chief technology officers, chief information security officers, or information security managers of an organization (Boynton, Zmud, & Jacobs, 1994).

Insider threat: An insider threat is a legitimate user within an organization who misuses privileges to perform an attack against the goals of the organization (Kaghazgaran & Takabi, 2015).

Perceived threat: The degree to which a person recognizes malicious IT as dangerous or harmful (Liang & Xue, 2010).

Risk: The measure of the extent to which an exceptional situation such as data security breach or failure affects business operations (Amundrud, Aven, & Flage, 2017).

Assumptions, Limitations, and Delimitations

This qualitative study included some assumptions, limitations, and delimitations. Graneheim, Lindgren, and Lundman (2017) explained that individuals see the world from their perspective. Researchers should appreciate and accept their underlying assumptions to remain as impartial as possible to improve the reliability of their study (Graneheim et al., 2017). A framework of the assumptions, limitations, and delimitations in this study follows.

Assumptions

Roulston and Shelton (2015) noted that no research study is free from the assumptions, biases, and personality of the researcher, and scholars cannot separate their nature from those activities in which they are involved. Assumptions are, therefore, certainties sighted as external factors that may reflect upon a researcher's inquiry (Semenova & Hassel, 2015). Twining, Heller, Nussbaum, and Tsai (2017) explained that assumptions surface when the general expectations of a researcher direct the investigative conclusion of a study. Therefore, individual interpretations or viewpoints may have shaped the path of this research. Thus, while conveying personal insights, researchers should provide reliable and supportive theoretical frameworks (Mortari, 2015).

In this study, I made several assumptions. I assumed that my participants provided accurate responses to my semistructured interview questions and that the data thus collated were an adequate representation of the strategies deployed by IT security managers in mitigating cybersecurity threats in their school districts. Ardagna, Asal, Damiani, and Vu (2015) recommended that researchers consider participants in qualitative research as experts in the areas relevant to the study. Therefore, I assumed that IT security managers who participated in my study had experience mitigating cybersecurity threats in their school networks. Another assumption was that the data collated were adequate to answer the research question.

Limitations

Limitations are potential weaknesses in a study and could be out of a researcher's control (Queirós, Faria, & Almeida, 2017). I anticipated some potential weaknesses emanating from the study, including the influence of study participants, my personal bias, sample size, and geographical constraints. Reliability, validity, and generalizability are essential limitations inherent in research (Berger, 2015; Boddy, 2016; Malterud, Siersma, & Guassora, 2016; Queirós et al., 2017). I selected a qualitative research method, which might have led to biases from my viewpoint and the experiences of my participants and therefore to biased and prejudiced opinions. Responses from study participants may have reflected views that were in the best interest of their organization or undermined their job inexperience, causing distorted results and wrong conclusions (Boddy, 2016). Malterud et al. (2016) noted that sample size and data availability might limit the reliability of research with a relatively large sample size that may yield a different result and conclusion of the research.

Another limitation was that IT security managers use different or multiple technologies, strategies, and procedures for monitoring online activities, which means that making any generalizations to school network security can be challenging. Still another limitation was that the study result may not be generalizable to the entire United

States, as the study was limited to the state of Texas. Finally, network, data breach, and cybersecurity are broad topics and may serve as a source of fear to students and school administrators in educational institutions. I limited this study to a focus on cybersecurity and data breach issues facing three school districts in Texas, as data collated for cybersecurity threats in one school district may differ from data assembled from participants in another school district.

Delimitations

Research delimitations are thoughtful mechanisms of applied research and refer to the exploration boundary or scope that researchers should establish before commencing a study (Rosenberg & Koehler, 2015; Semenova & Hassel, 2015). Rosenberg and Koehler (2015) reported that delimitations are factors that limit the scope of research and thus create boundaries of the study. Ardagna et al. (2015) documented that the lived experiences of participants are a significant delimiter. The interview questions were open-ended and the study included an interview protocol. I also considered the generalization effect of my research findings with a small sample size. Interviewing only IT security managers represented a delimitation because I would have otherwise interviewed other IT professionals who are not in the IT security position. A delimitation was that other IT professionals may provide relevant information on the complexity of data breaches in the school network within Texas. Another delimitation was the restriction to conduct the research only in Texas for convenience.

Significance of the Study

This study may be significant and valuable to IT security managers because I aimed to uncover strategies that organization leaders and IT security managers may leverage to mitigate data breaches on their school's network. Furthermore, I researched and initiated a more efficient and organized IT mechanism in institutions' networks that provides an IT threat-prevention system that may entail technology deployment; training to students; and more effective and appropriate IT guidelines, practices, and policies. Because the TTAT demonstrates the value of IT security, education, and awareness programs (Boss, Galletta, Lowry, Moody, & Polak, 2015), its use was of great worth to this study. An understanding of data breach could give district leaders and security administrators a higher sensitivity towards online security and provide a framework for implementing active online monitoring in school networks to mitigate data breaches and to obtain expert advice from internet safety partners. The theory thus serves as a model for IT security administrators to evaluate online threats and hence design effective cybersecurity solutions for both students and organizations.

Contribution to IT Practice

This study may contribute to IT security practice by providing information on how to reduce the number of potential cyber threats, data breaches, and other security incidents that students may encounter while surfing online. The research study may assist IT security managers in identifying and monitoring the activities of students using personal or assigned computing devices on their schools' networks. It may be especially crucial for managing students who intend to misuse the network system and expose themselves to cyber terrorism. This study may be valuable to IT security managers because of the security strategies proposed for circumventing these threats when perceived on a network. The research findings may also be important to IT security managers by providing a streamlined model for monitoring network resources and offering ways that may mitigate cyber threats on the internet.

The internet has become the ideal place for criminals and terrorists to carry out their actions and misdeeds. Therefore, cyber threats and other IT security threats such as data breaches have become two of the most significant risks to students using technology in Western societies (Pawlowski & Jung, 2015). The study may contribute to more efficient IT practice by providing solutions to the possible data breaches and cyber threats associated with online device usage and by offering strategies that will support the decision making and protection of students using technology for learning. A significant contribution from this study will increased security awareness and an improved strategic approach to threat mitigation, threat acceptance, and threat avoidance by understanding the needs and resources that require consideration in securing schools' networks using systematic implementation approaches.

Implications for Social Change

The research findings contribute to positive social change by creating awareness of insider security threats that students using technology for learning and communication may face from network security breaches and of appropriate security measures to inhibit the cyber threat process. The study results may also enable end users to understand how to handle cyber threats when they become victims by unknowingly opening a backdoor that attackers can use to break into their school-assigned IT devices. Additionally, the study findings may assist IT security managers, in identifying unique techniques and strategies on how to communicate and provide information to all users about potential and emerging threats to the business or organization information systems they monitor.

Furthermore, the findings could support IT security managers who enact safety precautions while managing schools' networks and technology. The study may lead IT security managers to develop online IT security training to improve IT threat awareness that could help students understand the need to use IT devices appropriately and that can subsequently prevent them from cyber threats. The research outcome provides information on how to protect students from the effects of cyber-attacks, offer a secure and nonthreatening online experience to students, and offer their guardians and families peace of mind while their wards use the internet for learning.

A Review of the Professional and Academic Literature

To conduct an encompassing literature review, I performed a critical analysis of various sources and content in the relevant literature, including reports, seminal books, presentations, and journals, from Google Scholar, SAGE, Walden's University Library, Elsevier, ProQuest, and some other scholarly databases. I extensively reviewed over 370 research sources for relevant material obtained via a search of key terms. The key words included *data breach, data security in education, network security and safety, risk management, internet misuse, security awareness, security governance, cybersecurity, threat, avoidance motivation, school network, online safety, coping, risk behavior, technology threat avoidance theory, security laws and regulations, school internet* *administration, data breach mitigation strategies*, *IT monitoring,* and *mitigation strategies on school networks.* I synthesized information from 175 resources for the literature review. Out of these, 168 resources (96%) were published between 2015 and 2019, 158 publications (90.2%) were peer-reviewed, six were government publications (3.4%), and 11 were non-peer-reviewed articles (6.2%). Numerous academic researchers have investigated cybersecurity strategies. The broad review of literature helps to establish a scholarly foundation for the study and was necessary to conduct a critical analysis of the body of knowledge related to the central research question: What strategies do IT security managers use to mitigate data breaches in their school's network? The objective of the literature review was to develop the conceptual framework.

Conceptual Framework

I chose the TTAT as the primary theory for this study based on a broad review of relevant literature relating to the fundamental research question on the strategies used by IT security managers in mitigating data breaches on schools' networks. Liang and Xue (2010) advanced the theory as a result of a synthesis of literature from vast areas of research, including risk analysis, psychology, information systems, and health care. With a basis in prior research on self-efficacy, psychology, risk analysis, and health-protective behavior, the TTAT emphasizes that the effectiveness of a chosen measure of safety, the cost associated with the applied action, and the degree of self-efficacy are the three dominant factors conceived by users when evaluating the extent to which a threat is avoidable (Liang & Xue, 2009). The TTAT is a theoretical framework that researchers can rely on for highlighting how IT managers can apply strategies to improve user safety on the internet and remain motivated to efficiently monitor student online activities in schools (Liang & Xue, 2009). Figure 1 illustrates the process of IT threat avoidance and shows the behavior of individual IT users when faced with a technology threat against an organizational level framework (Liang & Xue, 2009).

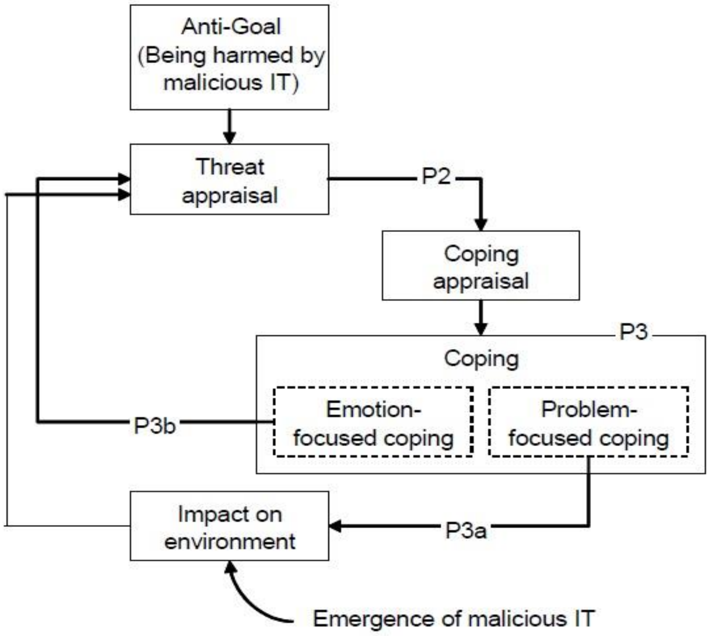


Figure 1. The process of IT threat avoidance. From "Avoidance of Information Technology Threats: A Theoretical Perspective," by H. Liang and Y. Xue, 2009, *MIS Quarterly, 33,* p. 77. Copyright 2009 by Liang and Xue. Adapted with permission (see Appendix D).

The process of IT threat avoidance theory hinges on the principle that users can avoid an IT threat when they perceive that a threat exists, by adhering to measures that will ensure their safety. Figure 1 further shows the processes and motives that influence individual users' IT threat avoidance behavior, which can be represented by a cybernetic process (Liang & Xue, 2009). The route to safety is for users to cope emotionally with a threat if they perceive that applying the available safety measures can avoid the risk (Liang & Xue, 2009). The TTAT also indicates why and how IT users are influenced to act in the event of a threat and adequately describes the factors and underlying processes that inspire their threat avoidance behaviors, drawing from the cybernetic and coping theories (Carpenter, Young, Barrett, & McLeod, 2019). Liang and Xue (2010) integrated both the process theory view and a variance theory view into the TTAT to incorporate the tests conducted by both process research and variance research methodologies. In process theory, TTAT describes IT users' avoidance behavior as a dynamic, positive feedback system that may begin with the advent of a threat state (Mitra, Guzman, Dhillon, & Tran, 2016). The threat state consequently extends to setting forth a state of being harmed once the user becomes aware of the threat (Young, Carpenter, & McLeod, 2016). If the cycle continues from the point where the user perceives that the current threat state is close to the set state of being harmed, the user will engage in coping mechanisms intended to expand the diminishing discrepancy between the threat state and the set state of being hurt, as shown in Figure 2 (Liang & Xue, 2010). Liang and Xue (2010) advanced the TTAT to describe individuals' cybersecurity behaviors regarding the motivation to avoid threats. The TTAT makes significant contributions to the literature on IT security, as users can achieve safety measures by avoiding the danger if they believe they can overcome a threat by acting thereof (Liang & Xue, 2009; Young et al., 2016).

Thus, the threat avoidance behavior continues until the threat disappears as the ensuing discrepancy becomes too large. The variance theory view provides essential variables that contribute to understanding threat appraisal, coping appraisal, and coping

(Young et al., 2016). According to the TTAT, individual IT users undergo two distinct cognitive processes: the threat appraisal and the coping appraisal. In threat appraisal, the existence and degree of a threat are appraised by the user, who subsequently decides what necessary measure to take to avoid it by using coping methods (Arachchilage, Love, & Beznosov, 2016). In using the TTAT, users can affirm that avoiding a threat and adopting technology are two qualitatively distinct phenomena. The position is exemplified given that the avoidance of risk is not similar to the acceptance of a protective measure, which indicates that the application of one theory, such as the preventive monitoring theory in a particular context, may lead to unreliable findings (Liang & Xue, 2009).

Furthermore, Liang and Xue (2010) submitted that, in the TATT, users could apply both problem-focused and emotion-focused coping approaches to reduce IT threats, as shown in Figure 1. Tu, Turel, Yuan, and Archer (2015) used the TTAT to examine the key factors that may affect end-user behaviors in avoiding and coping with cyber threats, as shown in Figure 2. The TTAT is thus a technique that IT security managers can use to practice evaluating system outcomes and subsequently be better at administering and securing school networks. The theory also identifies essential factors that expound the perception and motivation of users in the threat-handling process. Tu, Yuan, and Archer (2014) used the TTAT to examine the key factors that may affect end-user behaviors in avoiding and coping with security threats. School leadership should enact policies, design a security framework that consistently classifies information, act to counter threats, and ensure students' online safety (Boehmer, LaRose, Rifon, Alhabash, & Cotten, 2015).

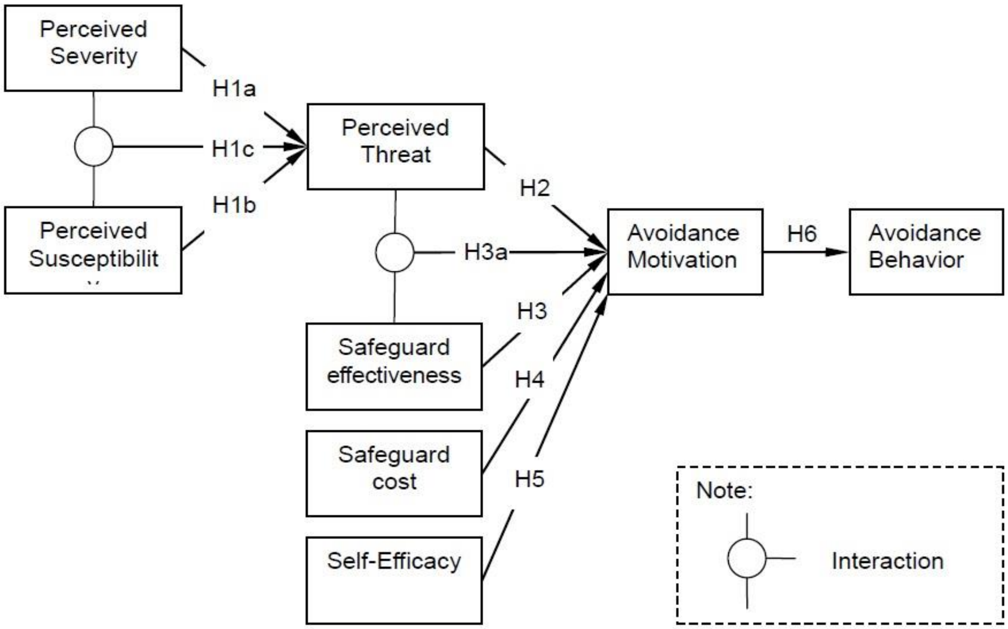


Figure 2. A research model signifying that motivation is influenced by an interaction between perceived threat and safeguard effectiveness. From "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective," by H. Liang and Y. Xue, 2010, *Journal of the Association for Information Systems, 11*, p. 397. Copyright 2010 by Liang and Xue. Adapted with permission (see Appendix D).

In Figure 2, TTAT shows why and how individual IT users are influenced to act when faced with a perceived threat and describes the factors and underlying processes that stimulate their threat avoidance behaviors by drawing stimuli from the cybernetic and coping theories (Fenner, 2017). In implementing the TATT, users can apply both problem-focused and emotion-focused coping approaches to reduce IT threats (Kashefi, Nuhu, Abbott, Ayoung, & Alwzinani, 2018). Figure 2 shows the research model that signifies that an interaction between perceived threat and safeguard effectiveness influences motivation (Liang & Xue, 2010).

Figure 2 shows the effectiveness of a chosen measure of safety, the cost associated with the applied standard, and the degree of self-efficacy in implementing the rule as the dominant factor is conceived by users when evaluating the extent to which the threat can be avoided (Arachchilage et al., 2016; Tu et al., 2015; Xu, Meso, & Ding, 2016). Figure 2 also shows a research model that signifies that motivation is influenced by an interaction between perceived threat and safeguard effectiveness (Liang & Xue, 2010). By leveraging this theory, IT security professionals can establish a more effective threat mitigation mechanism in which security depends on people's behavior toward avoiding the threat and on coping mechanisms more than on technical controls and countermeasures. Dang-Pham and Pittayachawan (2015) noted that by unknowingly opening a backdoor, attackers can break into assigned devices. With the diffusion of the internet, it has become easy for malicious IT users to exploit system vulnerabilities using viruses, trojan horses, botnets, worms, and spyware to amplify the negative impact. Information technology leaders have tested the TTAT against the context of antispyware software used to detect the presence of covert monitoring applications on a computer system (Liang & Xue, 2010; Tweneboah-Koduah & Buchanan, 2018; Young et al., 2016). According to the TTAT, users who are aware of the prescribed countermeasures and believe they have useful values can cope with threats and possibly avoid risks. Information technology security managers who secure district networks from data breaches can raise the security awareness level and can design processes to educate students about IT threats online while using the school's system inappropriately or unethically.

Analysis of Supporting Theories

The aim of the study was to explore the strategies used by IT security managers to mitigate data breaches on their network. The TATT is a theoretical framework frequently used for studying human behavior in the context of IT security (Liang & Xue, 2009). TTAT has made positive contributions to literature in IT security and to threat mitigation that internet users want to avoid an IT threat when they perceive that a threat exists, by adhering to measures that will ensure online safety (Arachchilage & Love, 2014). The TTAT shows how IT users cope with IT threats and the mechanisms that result in intentions and actual actions that mitigate the intended threats. The TTAT relates to other technology theories, such as the protection motivation theory (PMT), the theory of reasoned action (TRA), and the technology acceptance model (TAM).

Protection Motivation Theory

Researchers use the PMT to identify how individuals develop appropriate responses to technology threats. The PMT serves to predict individuals' intentions to protect themselves after receiving fear-arousing recommendations (Safa et al., 2015). Researchers can use the PMT to support the TTAT by determining how IT users not only perceive a threat and appraise its severity but also cope with it (Kostopoulos, Rizomyliotis, & Konstantoulaki, 2015; Liang & Xue, 2010). Both the PMT and the TTAT communicate countermeasures of how to avoid threats in information security (Kostopoulos et al., 2015; Liang & Xue, 2010). Jansen and van Schaik (2017) used the TTAT to explain individual online behavior and interactions when they perceive a threat. Steinbart, Keith, and Babb (2016) used the approach to measure specific decisions to maintain strong credentials for mobile internet devices when using the computer. The primary concerns of the PMT are the self-efficacy, safeguard effectiveness, and safeguard cost constructs. The PMT also serves as an approach or guide for computer users to evaluate system outcomes and subsequently understand information systems security issues (Kirichenko, Radivilova, & Carlsson, 2018).

Theory of Reasoned Action

The TRA includes a general framework for predicting behaviors related to technology adoption (Abraham & Sheeran, 2017; Montano & Kasprzyk, 2015). The TRA describes what causes individuals to develop intentions that predict users' behaviors towards technology (Ajzen, 2015; Montano & Kasprzyk, 2015). As technologies move to an online environment, it becomes increasingly important for researchers to factor in the concept of threat when attempting to explain the acceptance of those technologies. Jansen and van Schaik (2017) used the TTAT to explain precautionary online intentional behavior by individuals.

Technology Acceptance Model

The TAM is an additional construct in the TTAT model and includes avoidance motivation and avoidance behavior (Liang & Xue, 2010). Avoidance motivation refers to the user's level of motivation to avoid technology threats by implementing coping actions (Liang & Xue, 2010). TAM and TTAT support information systems theories that model how users come to accept and use technology. The primary concerns of the TAM are perceived usefulness and perceived ease of use, which are fundamentally relevant for computer acceptance behaviors (Arpaci, 2016; Kristadi & Sucahyo, 2016). In TAM, the user's primary intent is to have the liberty of choosing whether to avoid the difficulties associated with using technology spontaneously or compulsorily (Eltayeb & Dawson, 2016; Tarhini, Arachchilage, Masa'deh, & Abbasi, 2015) TAM emphasized users' behavioral plans to use or not use a specific technology by focusing on ease of use and usefulness (Eltayeb & Dawson, 2016; Kristadi & Sucahyo, 2016). Also, users' positive attitude toward specific technology leads to them developing an intention to use technology. The same goes for TTAT when users perceive that a threat exist such that they can either choose to cope with the threat or avoid it (Liang & Xue, 2010; Tu et al., 2015). The TAM excludes the fact that individuals can use information systems outside organizational settings and fails to address technology security (Arpaci, 2016).

Hence, TTAT is dependent upon avoidance behavior and emotion-focused coping that guard against malicious threats while using devices online, which has become a significant area for research. Liang and Xue (2010) contended that if a user's goal differs from the goal assumed by acceptance theories, then the explanatory powers of these theories are weakened. The TTAT appears to help IT security managers safeguard users against online attacks and provide an appropriate concept for understanding user avoidance habits and coping tendencies. Technology users can become victims of cyber threats when they compromise on security.

Analysis of Contrasting Theories

Technology threats are widespread in the IT sector, and IT security managers can mitigate these threats using different techniques. Liang and Xue (2009) developed the TTAT as a result of the shortcomings of the cybernetic theory and process theory.

Researchers use the TTAT to explain the IT threat avoidance of online vulnerabilities by technology users. Liang and Xue (2010) modified the TTAT to describe individuals' cybersecurity behaviors concerning their motivation to avoid threats.

The cybernetic theory is preferred for its consistency and for its wide acceptance as a theoretical framework for developing a better understanding of human behavior (Bliese, Edwards, & Sonnentag, 2017). Carver and Scheier (1982) clarified that the cybernetic theory is a general systems theory because it is identifiable with almost any mechanical system. Organizations in social, health, psychology, and organizational behavior theories have widely applied the principles of cybernetics in social, health, psychology, and organizational behavior theories (Bliese et al., 2017; Carver & Scheier, 1982; Klein, 1989). Nevertheless, the cybernetic theory, as earlier posited, encompasses a positive feedback loop. While the negative feedback loop concerns discrepancy reduction, the positive feedback loop acts to enlarge the discrepancy (Gadinger & Peters, 2016). The feedback loops increase the distance between the present state and the reference value specified by the goal.

The goal of the positive feedback loop is to identify an undesired end state that individuals endeavor not to achieve, referred to as antigoal by Gadinger and Peters (2016). In the positive feedback loop, a behavior is activated when the present state is too close to the undesired end state, and the act discontinues when the discrepancy is sufficiently large. The positive feedback loop describes the phenomenon that individuals avoid malicious IT, as also suggested by the TTAT (Arachchilage & Love, 2014). Using endpoint security solutions for IT mobile devices and encrypting e-mails are among many possibilities to mitigate security threats (Fernández-Alemán, García, García-Mateos, & Toval, 2015). According to Liang and Xue (2009), the central idea of cybernetics is that human beings self-regulate their behaviors by feedback loops. Although the process theory considers only the positive feedback loop in the TTAT framework, the cybernetic process hinges on both a negative feedback loop and a positive feedback loop (Carver & Scheier, 1982; Liang & Xue, 2009). Carver and Scheier (1982) posited that with TTAT, IT threat avoidance behavior could be represented by a cybernetic process in which users intend to increase the distance between their current security state and the unsafe end state by drawing on the cybernetic theory.

Tarhini et al. (2015) added that the TAM and theory of planned behavior do not work well in explaining mandatory IT usage because these theories generally refer to voluntary IT acceptance and usage. Markus and Robey (1988) extended the process theory for explaining user resistance to an information system. The process theory explained that users are likely to resist information system usage for varied reasons. Markus and Robey also explained the resistance to technology usage being due to several possible reasons: users may like the variations embodied in the system, users may become too apathetic to resist, or users may find ways to elude changes made to technology. The TTAT relies on the predicate that individuals can accept technology and moves beyond mere technology acceptance to establish how users behave in the face of threat either by avoidance or an emotion-coping method expressed in a feedback mechanism. In conclusion, the TTAT provides partial empirical support that accurately characterizes its approach to include a process model, a variance model, and many constructs that users can apply both problem- and emotion-focused coping to reduce IT threats (Boss et al., 2015).

Criticism of the TTAT

The TTAT does not cover all types of cybercrime mitigations, but rather a given section necessary to implement safeguards to avoid threats (Tarhini et al., 2015). According to the TTAT, avoiding a malicious threat is not the same as accepting a safeguarding measure based on two primary dependent constructs: the avoidance behavior and emotion-focused coping (Liang & Xue, 2010). Based on the assumption that avoidance and adoption behaviors are qualitatively dependent, applying one in a certain context may lead to inconsistency in another or even to false findings (Arachchilage & Love, 2014). The user's primary intent is to avoid the difficulty associated with using technology involuntarily when faced with risk, while in mandatory usage, the users do not have this liberty (Tarhini et al., 2015).

The outcome of using the TTAT presents itself in unpredictable user behavior and poor IT goal performance that leads to inconsistency from among the various IT security managers in improving network performance in this study. The TTAT thus suggests that IT security mangers should consider the purpose or valued outcome of IT usage in future IT acceptance research. However, until IT users accept and understand how technology works, it may be challenging to predict how individuals will behave when faced with technology threats.

Analysis of Potential Themes and Phenomena

In this section, I detail the techniques used to mitigate data breaches from which I draw possible themes. Also, I discuss potential issues in the literature related to strategies that IT security professionals may use to mitigate data breaches on their organization network. All organizations or institutions with electronic records hosted or accessible on the web, including education agencies, are vulnerable to security breaches (US Department of Education, 2017). Nearly half of all data breaches reported affect school districts. Mozumder et al. (2017) reported that a data breach can occur through a malicious or criminal attack, system malfunction, and human error (Privacy Rights Clearinghouse, 2016a). Workable strategies found to address these attacks on organization networks comprise an information security policy, people management, network security, an active password policy, antivirus protection and software update, physical security, audit, network security monitoring, data backup, intrusion detection, and security education training and awareness (Li, Tryfonas, & Li, 2016). Other potential themes include IT governance, standard continuity plan, IT leadership and policymakers, security laws and regulations, and security risk management.

Security controls can be technical, operational, and management instruments that protect the availability, integrity, and confidentiality of all IT infrastructures and their information (Hassanzadeh, Modi, & Mulchandani, 2015). IT security mangers use security controls to draw and segregate themes for better understanding. IT security managers who have the responsibility of administering and securing school networks from data breaches need to understand the various ways a data breach can occur and how to handle, avoid, or mitigate them as data grow in size and complexity within the system.

Applying technical security controls involves using technology to monitor and reduce vulnerabilities (Fink, Edgar, Rice, MacDonald, & Crawford, 2017). Technology security administrators install and configure technical controls to provide protection automatically and degrade system attacks (Hassanzadeh et al., 2015). Some automated tools include secure communication (virtual private network, secure sockets layer [SSL], Internet Protocol security [IPSec]), BitLocker, monitoring and intrusion detection systems (IDS), secure operations (antivirus software), firewalls, gateways, proxies, authentication, and device Identity and Access Management (restricting privileged user access). Using technical control implementation as a tool for systems hardening will improve the process of protecting and safeguarding personal data, securing high-risk organizational information, and condensing surface vulnerabilities (Fink et al., 2017).

Secure Data Communication (Encryption)

Encrypting data is one of the most effective ways to help keep data secured (Goyal, 2016). According to Kuypers, Maillart, and Pate-Cornell (2016), incidents can occur from lost or stolen devices, such as tablets, phones, or laptops, that contain sensitive data. Such events require varying levels of investigation, depending on the encryption level of the device and the type of equipment. Warding off or minimizing conflict requires that devices accessing a network are encrypted in a secured format to prevent IT threats (Subedi, Budhathoki, Chen, & Dasgupta, 2017). The BitLocker encryption feature is an innovative security strategy issued by Microsoft for Windows operating system drivers that protects data by encrypting complete volumes (Goyal, 2016; Meijer & Van Gastel, 2019). The adoption and implementation of cybersecurity laws, as well as certificate-based protocols to integrate with access control systems, layered encryption, and third-party security providers, can assist in providing a robust and scalable network security management module for managing devices across organizations (Mushtaq et al., 2017).

BitLocker. BitLocker protects machine data in the event a computer is stolen or lost by securing it using a PIN code that requires generation every time the operating system reboots (Goyal, 2016; Lewis & Palumbo, 2018) This method of encrypting a system hard drive is advantageous in cases where an intruder or attacker succeeds in stealing a computer system or gains access to a lost system (Goyal, 2016; Lewis & Palumbo, 2018; Meijer & Van Gastel, 2019). The BitLocker encryption technique makes the data unreadable, unrecognizable, and unrecoverable without PIN code authentication (Goyal, 2016; Meijer & Van Gastel, 2019). The data encryption key of the BitLocker stores a trusted platform module that performs cryptographic operations (Goyal, 2016; Lewis & Palumbo, 2018).

Encryption software uses cryptography, the Advanced Encryption Standard algorithm in cipher block chaining, or XEX-based tweaked-codebook with ciphertext stealing (XTS) mode with a 128-bit or 256-bit key to prevent unapproved access to digital information (Adamovic, Sarac, Stamenkovic, & Radovanovic, 2018; Braga & Dahab, 2015; Lewis & Palumbo, 2018; Meijer & Van Gastel, 2019). Cryptography serves to protect digital data on computer devices and other networks over the internet

(Adamovic et al., 2018; Braga & Dahab, 2015; Daman & Tripathi, 2015). A cipher (asymmetric and symmetric keys) uses encryption as a tool to conceal the content of message in a particular way only the sender and receiver can understand using secret keys (Braga & Dahab, 2015). The main security goal of using encryption software is to secure or preserve the integrity, authenticity, confidentiality, and nonrepudiation of information (Braga & Dahab, 2015). The drawbacks associated with this technique are the time-consuming process, the risk of misremembering the recovery key, the lack of data protection against network attacks, and the lack of security when the system is on and left unattended (Goyal, 2016; Lewis & Palumbo, 2018). Internet Protocol security, Secure Copy protocol (SCP), secure e-mail, secure shell (SSH), SSH File Transfer Protocol, and other secure web communication protocols such as Hypertext Transfer Protocol Secure rely on some encryption for users' data protection. Network security has become more critical with the increase in internet use, connectivity, and communication among devices (Khan & Goodridge, 2019).

Secure shell. A protocol outlines how cryptographic algorithms can secure information (Adamovic et al., 2018; Braga & Dahab, 2015; Daman & Tripathi, 2015; Harchol, Abraham, & Pinkas, 2018). SSH typically provides secure channels over an unsecured network using cryptography (Adamovic et al., 2018; Braga & Dahab, 2015; Daman & Tripathi, 2015).

Internet Protocol security. The IPSec policy consists of lists of rules that designate how network traffic can be protected using virtual private networks (Al-khatib & Hassan, 2018). The IPsec policy includes protocols for establishing mutual authentication between clients and agent machines at the start of a session and by negotiating which cryptographic keys to use during the session (Adamovic et al., 2018; Al-khatib & Hassan, 2018; Braga & Dahab, 2015; Daman & Tripathi, 2015). The cryptographic security service protects its users when they communicate over Internet Protocol by supporting its network-level peer authentication, data origin authentication, data integrity, data confidentiality, and replay protection (Adamovic et al., 2018; Al-khatib & Hassan, 2018; Braga & Dahab, 2015; Daman & Tripathi, 2015). When users have installed these services and use them correctly, IPsec can protect data flows between network devices, security gateways, or host machines on the network. Thus, IPsec has become the standard security protocol for securing internet communications and providing traffic integrity, confidentiality, and authentication (Alam & Hamid, 2018; Hassanzadeh et al., 2015). For IPsec to function effectively, its configuration policy must be analyzed for consistency across the entire organization network (Alam & Hamid, 2018; Hassanzadeh et al., 2015).

Secure Copy protocol. A critical challenge in modern technology involves securing end-to-end network communication and improving performance during data transfers (Nguyen, Ghosh, & Krishnamachari, 2018; Nkenyereye & Jang, 2017). The SCP assists client machines in the safe copying of files between a local and a remote computer. IT security administrators are posed with the responsibility of ensuring data are secured when transferring computer files between a client machine and a remote network device or between two remote network devices (Nguyen et al., 2018; Nkenyereye & Jang, 2017). Secure Copy protocol are two communication host entities that do not want a third party to listen in using the same mechanisms for authenticating client machines, thereby ensuring the integrity and confidentiality of the data in transit (Jackman et al., 2019; Nguyen et al., 2018; Nkenyereye & Jang, 2017). The client machines can also request files or directories from a server by downloading them in a secure manner (Jackman et al., 2019; Nguyen et al., 2018; Nkenyereye & Jang, 2017). Although technology experts may find secure host protocol outmoded, more modern protocols like SSH File Transfer Protocol and Remote Sync are suitable for securing networks during file transfers (Jackman et al., 2019; Nkenyereye & Jang, 2017).

E-mail encryption. Endpoint security solutions for mobile devices and encrypted e-mails are among many other possibilities for mitigating security threats (Fernández-Alemán et al., 2015). One of the means of communication using technology in most organizations is exchanging e-mails transmitted across networks, and such communication is often unencrypted (Durumeric et al., 2015; Foster et al., 2015). As e-mails sent across the networks are prone to the disclosure of information, there is a need for e-mail encryption to include authentication. STARTTLS is a typical e-mail encryption extension tool that uses Transport Layer Security (SSL) layer rather than plaintext communication, which allows organization e-mail servers to upgrade their plaintext communication to encrypted connections across devices (Durumeric et al., 2015; Foster et al., 2015). E-mail encryption is an application security control that provides technology users the assurance that information sent across network devices is safe and accessible only by authorized persons (Daman & Tripathi, 2015; Fernández-Alemán et al., 2015; Foster et al., 2015). Hence, the encryption of e-mail messages is meaningful and designed to protect the content of information from being read by entities other than the intended recipients (Daman & Tripathi, 2015; Fernández-Alemán et al., 2015).

SSH File Transfer Protocol. The SSH File Transfer Protocol provides secured file access and file management over any reliable network stream (Adamovic et al., 2018; Braga & Dahab, 2015; Daman & Tripathi, 2015; Harchol et al., 2018). The SSH File Transfer Protocol includes an assumption that any data running on a client machine over a secured channel has already been identified and screened, and so authentication can easily follow (Adamovic et al., 2018; Braga & Dahab, 2015; Daman & Tripathi, 2015; Harchol et al., 2018).

Hypertext Transfer Protocol Secure. IT professionals have come to understand that the Hypertext Transfer Protocol could cause many risks to users if data transmitted across networks are unsecured and unencrypted (Dimitrova & Mileva, 2017; Suharyanto, 2017). Persons with authorized access to a system can read and alter unencrypted data sent over an unsecured network (Dimitrova & Mileva, 2017; Suharyanto, 2017). The Hypertext Transfer Protocol Secure uses a secure communication protocol encrypted using Transport Layer Security with standard port 443 over a computer network (Dimitrova & Mileva, 2017; Suharyanto, 2017).

Monitoring and Intrusion Detection System

Cybersecurity control consists of all the methods IT security experts can use to protect the reliability, integrity, usability, consistency, and safety of data, programs, and entire computer networks from criminal access that are vulnerable and can be leveraged for malicious activities (Czuprynski & Smith, 2017; Mishra, Goel, & Virbahu Jain, 2017). Information technology monitoring control tools can also include administrative techniques and operational controls as strategies for mitigating data breaches and cybersecurity controls (Czuprynski & Smith, 2017; Mishra et al., 2017). A monitoring instrument for networks and computer systems such as the IDS can lead to an increase in IT quality and network performance when used to identify vulnerabilities and protect the information assets of an organization from malicious attacks (Venkatraman, 2017). The activities of unauthorized or inappropriate system activities can go undetected when there is a failure in the monitoring and detection system. (Frank & Wagner, 2018).

Using a cloud-based network management administration solution can help streamline remote network attacks, can help control devices, and can help users across an entire organization network (Makhdoom, Abolhasan, Lipman, Liu, & Ni, 2018). At a minimum, IT professionals who are responsible for online safety should log and monitor all significant events, including access to and modification of sensitive or critical system resources. Spam e-mails sent in bulk may result in organization network congestion; hence, a need exists for active system log analyzers and monitoring (Dev & Liu, 2017; Tuor, Kaplan, Hutchinson, Nichols, & Robinson, 2017). To simplify network management tasks via a centralized web console, pushing out software updates can help present a case on how best to respond actively to IT threats and provide normative guidelines to the practical use of deployed IT systems (Pereira, Barreto, & Amaral, 2017; Shameli-Sendi, Aghababaei-Barzegar, & Cheriet, 2016). If a computer network has the right IDS in place, an attacker who is skilled at accessing unauthorized networks may be walled off by the most valuable technique in place such that the attacker's presence can be automatically detected and can kick the attacker out of the system as quickly as possible (Tracey, O'Sullivan, Lane, Guy, & Courtemanche, 2017). Scanning networks and systems can help to minimize any exposure to known vulnerabilities (Kumar & Kumar, 2016; Makhdoom et al., 2018; Young et al., 2016).

Secure Operation (Antivirus Software Tools)

Information technology security managers may use a spam monitoring tool to analyze and monitor spam, and they may use logs to form a foundation to explain patterns in user behavior (Dev & Liu, 2017). Zhang and Gupta (2018) and Arachchilage et al. (2016) listed some common online attacks and threats, which included computer viruses and malicious software (malware), social engineering and online identity theft (phishing), unsolicited e-mail (spam attack) and eavesdropping software (spyware). Others include impersonation, hijacking, image retrieval and analysis, and distributed denial-of-service attacks (orchestrated campaigns aimed at making computer resources unavailable to intended users). Information technology security managers need to implement a robust IT spam monitoring tool in real time. Real-time monitoring can help security professionals in decision making, enhance safety and productivity, help determine the behavior of a network and the status of its components, and reduce operational costs (Benjelloun & Lahcen, 2019).

Firewalls, Gateways, and Proxies

Firewalls, gateways, and proxies are network security monitoring devices that help control traffic on networks based on some defined security rules (Chopra, 2016). Firewalls mainly authenticate barriers between an internal trusted network and an external untrusted network to identify behavioral intention patterns as strategies that can help organizations build an in-depth knowledge about how to reduce potential security and privacy incidents across an organization network (Bello Garba, Armarego, & Murray, 2015). Computer gateways serve as access points to another system or an internet service provider that connects end users to the internet (Chopra, 2016). A gateway firewall help organizations route network traffic and secure networks by protecting its network resources through filtering messages at the application layer from one computer workstation to the outside system (Chopra, 2016). Without setting up these systems properly, cyber attackers can turn organization devices into zombie devices and use them to create botnets to attack other users' communication and personal devices, including the organization network authentication protocols configured on these devices (Shameli-Sendi et al., 2016).

Another way of securing network resource is by shutting down all applicable services and ports attacked within the computing environment at any time (Kumar & Kumar, 2016; Makhdoom et al., 2018; Young et al., 2016). Proxies also work as firewalls in the sense that they block an organization's network devices from being open to the internet by redirecting web traffic when necessary (Chopra, 2016; Kumar & Kumar, 2016; Makhdoom et al., 2018; Young et al., 2016). In a network computer environment, a proxy server acts as a server intermediary for requesting information from clients and seeking resources from other servers (Chopra, 2016; Kumar & Kumar, 2016; Makhdoom et al., 2018; Young et al., 2016). Whereas firewalls can block ports and programs that try to gain unauthorized access to organization computers, proxy servers will try to hide internal organization networks from the internet (Chopra, 2016; Kumar & Kumar, 2016; Makhdoom et al., 2018; Young et al., 2016). The proxy servers are similar to application-layer gateways in that the servers implement security at the application layer based on individual protocols such as HTTP and File Transfer Protocol (Chopra, 2016; Dimitrova & Mileva, 2017; Suharyanto, 2017).

Authentication and Device Identity and Access Management (Restricting Privilege User Access)

Without authenticating and limiting user access to different network devices from multiple locations at the same time, a data breach can occur that may defile the confidentiality, integrity, and availability of data and the system (DiMase, Collier, Heffner, & Linkov, 2015). Managing user access is another control strategy that can help maintain a network that deters both malicious and negligent threats (Lal, Taleb, & Dutta, 2017). An organization network security team may authenticate user access to resources and other network applications by implementing adequate controls that restrict multiple sign-ons from one location at any given time as a strategy for mitigating a breach (Lal et al., 2017). IT security experts should also limit access to sensitive data to only those who need such information to fulfill their job duties (Czuprynski & Smith, 2017; Mishra et al., 2017). Users who have access to confidential personal data should be authenticated using the right tools and forced to use secure passwords and other methods of authentication to access the data (Czuprynski & Smith, 2017; Mishra et al., 2017).

In monitoring accounts and authorizing privilege access rights, IT security managers should periodically identify, evaluate, and review user access to data and other information resources to ensure the user access rights remain appropriate and are commensurate with their assigned responsibilities. As users change positions and job descriptions change within an organization, access rights to systems should be added, modified, or removed (Thomas & Galligher, 2018). Without proper monitoring, users may hold access rights that are no longer necessary, thereby increasing an organization's risk of unauthorized access to data (Thomas & Galligher, 2018).

Server authentication. IT security experts should allow technology users to have some level of confidence in the way they communicate with devices (Chaudhry, 2016; Odelu, Das, & Goswami, 2015; Suharyanto, 2017). Users should be aware that technology is not always safe and that a need exists to ensure they are in the right environment and communicating with the right person and the right technology, which creates more room for confidentiality or integrity (Chaudhry, 2016; Odelu et al., 2015; Suharyanto, 2017).

Data confidentiality. Data confidentiality relates to the integrity of data running between the end user's browser and the webserver if the data running through it are encrypted and it becomes impossible for an eavesdropper to discern the content of the communication (Darwazeh, Al-Qassas, & AlDosari, 2015; Yan, Wang, Li, & Vasilakos, 2016). Authentication is necessary for implementation on network devices such as e-mail servers, where both the sender and the recipient support an encrypted communication such that any eavesdropper who can access the interaction between the mail servers cannot use a sniffer tool to see the e-mail contents (Darwazeh et al., 2015; Yan et al., 2016).

Data integrity. The ability of a nefarious network user to modify, distort, or destroy data transmitted between the user's browser and the webserver due to implemented encryption and cryptography depends on the level of data integrity (Braga & Dahab, 2015; Subedi et al., 2017). The primary motive for accessing and authenticating a website is to ensure the protection of users' data for the sake of privacy and integrity while data are exchanged and in transit (Braga & Dahab, 2015; Subedi et al., 2017). Data integrity protects against man-in-the-middle attacks (Vanhoef, Bhandaru, Derham, Ouzieli, & Piessens, 2018). The bidirectional encryption of communications between a client and a server protects against eavesdropping and tampering of the connection to ensure data integrity (Braga & Dahab, 2015; Subedi et al., 2017; Vanhoef et al., 2018). In practice, data integrity provides a reasonable assurance that devices are communicating to the right website without any fear of interference posed by imposters.

Operational security controls. Operational security controls serve to support organizational infrastructure and its security managers in ensuring the daily operations of an organization comply with the company’s overarching IT security plans, goals, and objectives (Hassanzadeh et al., 2015). Some of the operational controls for consideration in this study include IT security awareness and training, configuration and change management, incident response and contingency planning, media protection, and physical and environmental protection.

IT Security Awareness and Training

In implementing strategies that prevent a data breach, the human aspect is an important aspect, as it is one of the causes of information security incidents (Ghazvini &

Shukur, 2016). Human errors are a critical factor in information security assurance, and a formal security and awareness training program can help minimize their impact (Da Veiga & Martins, 2015; Dhakal, 2018; Ghazvini & Shukur, 2016). Most IT security experts agree that humans are the weakest link in defense of information integrity within organizations (Czuprynski & Smith, 2017; Ramalingam, Khan, & Mohammed, 2016; Soomro et al., 2016). Although a significant number of institutions never carry out continuous security training to help employees spot cyber-attacks, many others do so only when new employees join the company or when there is an incident or an IT threat (Czuprynski & Smith, 2017; Ramalingam et al., 2016; Soomro et al., 2016). Users' ignorant and negligence of information security practices and lack of awareness and training are some of the fundamental causes of data breaches (Palinkas et al., 2015; Ramalingam et al., 2016). Many IT security leaders provide security awareness training, but there is a concern regarding why the training is not working (Czuprynski & Smith, 2017; Safa et al., 2015).

The lack of awareness training programs can influence the information security practices of organizations (Bello Garba et al., 2015). IT leaders that have chosen to accept bring-your-own-device programs on their network prefer mobile devices, because the organization benefits from lower corporate costs, less technical training, and increased productivity without considering the risks (Bello Garba et al., 2015). One way to address the human aspect is to annex information security education programs to users' periodic work ethic requirements as a way to improve their knowledge of security threats, which will contribute to the protection of IT organization assets (Da Veiga &

Martins, 2015; Halaseh & Alqatawna, 2016). Well-defined information security training is necessary to enhance users' knowledge, which will lead to a secure user behavior in the mitigation of online security threat (Czuprynski & Smith, 2017; Furnell & Vasileiou, 2017; Safa et al., 2015). Online security awareness training, workshops, security awareness posters, newsletters on security, and meetings are some of the ways IT security managers and leaders can improve users' knowledge of information security (Dhakal, 2018; Safa et al., 2015). Da Veiga and Martins (2015) noted that regulatory requirements are necessary to improve the information security culture in organizations such that the behavior of the workforce complies with information security and related information processing policies.

To protect online users from data breaches, IT security leaders ought to educate users on the need to avoid online dangers when they see them (Hall, Schmader, Aday, & Croft, 2019). Training approaches can be nontechnical solutions that can help mitigate IT security threats and phishing problems (Dhakal, 2018; Ghazvini & Shukur, 2016). Dey, Ghoshal, and Lahiri (2018) recommended that security training be enforced and designed in ways that attract users' attention to enhance awareness and help them retain the knowledge acquired.

Educating users and creating security program awareness is a strategy needed to achieve the best security practice and can be an invaluable resource for tracking down the source of an attack on a network (Al-Daeef, Basir, & Saudi, 2017; Wash, Rader, Berman, & Wellmer, 2016). School district leaders and IT security managers given with the responsibility of protecting a school network need to complete a comprehensive information security training program in which they learn to give security threat awareness training precedence over everything else. Security leaders used TTAT to determine whether users are less likely to carry out additional precautionary authentication procedures when accessing the web if they believe they have the knowledge to cope with threats than those who think they are not capable (Fenner, 2017; Liang & Xue, 2010). To understand users' security training requirements, stakeholders need to identify and research individual users' positive and negative feelings toward training and the factors required to understand effective security awareness programs (Furnell & Vasileiou, 2017). There is, therefore, an increasing acceptance that online users need to have some degree of knowledge of the roles they can play in accessing and keeping an organization's data secured. Awareness training programs should include information for users on potential threats, emerging vulnerabilities, and their challenges concerning the business model.

Configuration and Change Management

Configuration management often involves using a baseline to ensure systems start in a secure, hardened state (Boutin, 2015; Josey, 2016; Khan, Azam, Anwar, & Kiran, 2019). Change management helps ensure that changes do not result in unintended configuration errors (Boutin, 2015; Josey, 2016; Khan, Azam, et al., 2019). Configuration and change management (CCM) is an operational control for maintaining and managing the integrity of the hardware, software, firmware, and all documentation related to the CCM process in the project development process (Boutin, 2015; Josey, 2016; Khan, Azam, et al., 2019). The purpose of CCM is to establish a means to ensure the integrity of assets using change control and change control audits (Boutin, 2015; Josey, 2016; Khan, Azam, et al., 2019).

Changes occur within an organization’s IT environment for different reasons. It could be to harden the network system, deploy software patch updates, back up data files, configure a new system, roll out new versions of software, or decommission an old system for a new (Boutin, 2015; Josey, 2016). Information technology managers should reduce the frequency of rolling out changes so that it does not affect the totality of the business process, which makes it hard to assess authorized changes on the impact of operations and security within the IT environment (Boutin, 2015; Jayatilleke & Lai, 2018; Josey, 2016; Morozov, Kalnichenko, Timinsky, & Liubyma, 2017; Park, 2018). Only qualified and licensed users should be allowed to change any network configurations if their roles and responsibilities have changed and are defined in accordance with business documentation (Boutin, 2015; Jayatilleke & Lai, 2018; Josey, 2016; Morozov et al., 2017; Park, 2018). IT security personnel can request an emergency change within a configuration item for any information resources, such as routers, operating systems, or firewall configurations, or to correct an existing error in a database server to avoid data integrity before making such changes (Boutin, 2015; Jayatilleke & Lai, 2018; Morozov et al., 2017).

Configuration and change management is a continuous process of testing and supporting improvements to information assets or related infrastructure that support the critical services of a business (Jayatilleke & Lai, 2018; Josey, 2016; Morozov et al., 2017; Park, 2018). The method includes the addition of new assets, changes to assets, and the exclusion of assets (Jayatilleke & Lai, 2018; Josey, 2016; Morozov et al., 2017; Park, 2018). A configuration management system maintains one or more configuration databases, and each database stores attributes of configuration items and their relationships with other configuration items (Jayatilleke & Lai, 2018; Josey, 2016; Morozov et al., 2017; Park, 2018). A configuration management database contains details such as servers, code modules, applications, and other items in a database about how they are connected throughout their IT life cycle (Boutin, 2015; Josey, 2016; Khan, Azam, et al., 2019). As the complexity of IT systems increases, the complexity of the methods used to create these IT systems also grows, as does the likelihood of unexpected failures in configuration (Boutin, 2015; Josey, 2016; Khan, Azam, et al., 2019). The impact of these glitches puts data and systems that may be critical to business operations at a notable risk of failure that could cause an organization to lose business, suffer damage to its reputation, or close completely (Boutin, 2015; Josey, 2016; Khan, Azam, et al., 2019).

Information technology security managers should understand that having a CCM process to protect against these errors is significant to the overall security posture of the organization. To manage and improve organization IT systems effectively, IT professionals need to know what assets are in their IT environment and which one has the current and accurate configuration data (Jayatilleke & Lai, 2018; Josey, 2016; Morozov et al., 2017; Park, 2018). With an accurate configuration management database, it is easy to understand an organization’s IT environment, particularly in the areas of service impact analysis, asset management, compliance, and configuration management (Jayatilleke & Lai, 2018; Josey, 2016; Morozov et al., 2017; Park, 2018). A configuration management database also provides users with a set of configuration data list a means of examining all the data from any desired perspective. Executing a change management process includes all the steps, from change identification to change request, request review, prioritization by the change review board, evaluation through impact analysis, change approval or rejection, change testing, implementation and postimplementation review, and request closing (Jayatilleke & Lai, 2018; Josey, 2016; Morozov et al., 2017; Park, 2018).

According to Jayatilleke and Lai (2018), and Park (2018), to execute a change control configuration process, the following integrative steps are necessary for users to justify the proposal: test, implement, review, update (whether upgrade or modification), and audit the information system change. IT administrators can either modify or roll back changes that do not occur as planned (Boutin, 2015; Jayatilleke & Lai, 2018; Josey, 2016; Morozov et al., 2017; Park, 2018). For CCM, as with many activities, planning affects the success or failure of a project (Boutin, 2015; Morozov et al., 2017; Park, 2018). Before implementing any change control, tests should be performed, preferably in a preproduction environment (Boutin, 2015; Jayatilleke & Lai, 2018; Josey, 2016; Morozov et al., 2017; Park, 2018). A production environment that reflects reality must also make sure that the tests are transferable to the operational environment (Boutin, 2015; Jayatilleke & Lai, 2018; Josey, 2016; Morozov et al., 2017; Park, 2018).

Incident Response and Business Contingency Planning

Every day, IT security experts cope with the flow of cybersecurity incident resolution (Kuypers et al., 2016). Although most events trigger some routine feedback, others require a large effort to probe further and resolve (Kuypers et al., 2016). However, security operation teams in organizations need to continue to proffer responses to issues requiring their expertise on security threat issues that could remain unclear to the end-user (Kuypers et al., 2016). As IT security professionals collect cybersecurity incident data files for IT audit, compliance, and management, they can leverage the information available to derive risk metrics, which in turn may lead to more informed security investments (Kuypers et al., 2016). According to Kuypers et al. (2016), different incidents can occur, including the following:

- Organization information spilling out to unauthorized individuals, such as when users send an e-mail containing sensitive information, such as employee social security numbers, to unauthorized persons (data spillage).
- An intrusion or an attempted phishing attack on users and their machines, such as when hackers gain access to valid users' e-mail account credentials to spam other users or attach a malicious file to infect other users' machines with malware (e-mail incident).
- Lost or stolen devices, such as tablets, phones, or laptops, which will require a different level of investigation depending on the encryption level and the type of equipment.
- Intercepting IT tasks carried out online, which can include log pulling, patching, or e-mail archive investigation, which is meant to aid auditing.

- A web attack where hackers gain access to an organization’s website via a Structural Query Language (SQL) injection, a compromised server, or defacement.
- Users browsing a compromised website, downloading malware while visiting a site, and spreading it using a USB device. Malware that does not originate via e-mail or through a website is categorized as a web browsing/USB incident.
- Denial of service and false alarms, are other incidents can could occur.

Responding to these incidents involves allocating the right resources to tackle the frequency of the occurrence and the severity of the event measured by person-hours (Kuypers et al., 2016).

Business continuity includes several different methods that help stakeholders plan and prepare for potential system outages. The goal is to reduce the overall impact on the organization if an outage occurs. Accepted conventional continuity planning or a suite of detailed incident response plans should be developed for restoring critical business functions and applications promptly (Tracey et al., 2017). Therefore, standard business continuity planning is paramount in every organization to ensure emergency plans are in place during a disaster that does not disrupt IT core business operations (Tracey et al., 2017). Business continuity planning involves using the predict-and-prevent strategy to promote organization resilience that will enhance persistent organization capacity and maintain business operations during a disaster (Tracey et al., 2017). Organizations that are resilient will be able to resist, absorb, recover, and adapt to the adjusted environment following a crisis. Business continuity planning is essential not only for ensuring the availability of IT systems and services but also for maintaining IT infrastructure, maintaining efficiency in supply chains, and ensuring stability within the system (Tracey et al., 2017). Business continuity planning leaders need to be able to adopt and promote preparedness strategies by creating awareness; communicating information correctly; and providing human resources, physical support, and social capital (Tracey et al., 2017).

Business continuity planning allows for the development of a comprehensive continuity plan and formally assigns responsibilities for the event, implementation, and maintenance of the program to appropriate personnel (Tracey et al., 2017). District leaders may establish and document an incident response plan that centrally tackles all security incidents with implementation. Without tested and functional business continuity planning, management may have limited assurance that an organization’s business functions correctly and that computer processes can be sustained during or after a disruptive incident (Tracey et al., 2017). The strategy can assist the incident response team in carrying out an extensive security audit on how to address IT threats and damage done to the network (Tracey et al., 2017).

Media Protection

Media devices include such items such as compact discs, flash drives, magnetic tapes, external or removable hard disk, and digital video disks (Hendre & Joshi, 2015; Kalaiprasath, Elankavi, & Udayakumar, 2017). Media protection encompasses the protection of content inside media devices, including music, movies, and software (Kalaiprasath et al., 2017). A system backup is a systematic approach for conducting system data recovery, risk assessment, and threat vulnerability evaluations (Sohail &

Venugopal, 2017; Thomas & Galligher, 2018). A media protection establishes a program for an appropriate media backup and storage, which may entail performing a consistent system backup, storing the backup media files properly in an offsite location, and encrypting the media content in a secure format to reduce IT security threats (Subedi et al., 2017). To avoid data loss and sustain business continuity, IT security managers need to ensure proper backup policies are in place. Data breaches and cyber threats can be mitigated or prevented from unauthorized access to backup volumes when privileges are threatened, and corrupted data can be recovered from the backup disk (Subedi et al., 2017).

The purpose of media protection is to control risks from media access, storage, transport, and protection that lead expectedly to a valid media security program (Force, 2017; Khou, Mailloux, & Pecarina, 2017; Ren, Chen, & Zhang, 2018). Hence, a need exists to consistently monitor and evaluate media (Force, 2017; Khou et al., 2017; Ren et al., 2018). According to the U.S. Environmental Protection Agency (EPA), the media protection program allows an organization to comply with the standard policy in addition to the effective management of all media that contain sensitive and nonsensitive information from commencement through to destruction (U.S. Environmental Protection Agency, 2019).

Media protection policy and procedures. IT leaders can adopt or develop and maintain a media protection program that includes the implementation of the media protection policy and associated controls with an annual review of the plan (Force, 2017; Khou et al., 2017; Ren et al., 2018).

Media access restrictions. Access to sensitive information may be restricted to authorized individuals (Hendre & Joshi, 2015; Kalaiprasath et al., 2017). Limiting access to digital media includes restricting access to organizational design specifications stored on compact disks in the media library (Force, 2017; Khou et al., 2017; Ren et al., 2018).

Media storage. IT security administrator's may store all sensitive media in a secured, access-controlled area and protect the media until ready to be destroyed or sanitized using organization-approved equipment, techniques, and procedures (Force, 2017; Khou et al., 2017; Ren et al., 2018).

Media transport. Secure encryption is necessary to protect the integrity and confidentiality of sensitive media during transport outside of controlled areas (GSA-IT, 2020; Kumar, 2015; U.S. Environmental Protection Agency, 2019). Activities associated with the transportation of such media must be restricted to authorized personnel. Encryption provides data protection, while a critical management tool enables access to protected data. It is justifiable to encrypt data in transit over networks, at rest, and on backup media (GSA-IT, 2020; Kumar, 2015; U.S. Environmental Protection Agency, 2019).

Media sanitization. IT security administrators must sanitize sensitive media, both digital and nondigital, before disposal, reuse, or release out of organizational control (Force, 2017; Khou et al., 2017; Ren et al., 2018). Regenscheid, Feldman, and Witte (2015) noted that clearing, purging, destroying, and cryptographic erasure are techniques and actions used to sanitize electronic media.

Media use. Security leaders may restrict the use of portable storage devices for its IT environment to implement security measures (Force, 2017; Khou et al., 2017; Ren et al., 2018). The use of removable or portable media devices may be restricted to an organization's environment when necessary (GSA-IT, 2020; U.S. Environmental Protection Agency, 2019). Methods of limiting access to media include, but are not limited to, disabling, or physically blocking ports, approved devices, and device types (GSA-IT, 2020; U.S. Environmental Protection Agency, 2019). Unknown removable media or removable drives should never be connected to or inserted into any system without following organization media policy (GSA-IT, 2020; U.S. Environmental Protection Agency, 2019). All personal devices may be treated as malicious until verified by the security administrators (GSA-IT, 2020; U.S. Environmental Protection Agency, 2019). Also, personally identifiable information should never be stored on removable media (Schmidlin, Clough-Gorr, & Spoerri, 2015). If personally identifiable information is stored on removable media for organization business, then IT leaders must use and validate secure encryption (Schmidlin et al., 2015).

Physical and Environmental Protection

Physical protection controls consist of cameras, door locks, and environmental controls such as heating and ventilation systems (Kumar, Vealey, & Srivastava, 2016). Physical security controls for IT assets and operations should protect the physical layers of IT infrastructures like local computers and servers, storage media, printers, scanners, copiers, and multifunction devices, which are often overlooked in a rush (Kumar et al., 2016). To prevent situations of data incidents where intruders can gain access to environmental organizations’ data center and network infrastructure, then video surveillance or alarm bells are necessary to prevent theft (Makhdoom et al., 2018). Security entry access codes and locks for buildings or rooms containing sensitive information need to be changed periodically (Fink et al., 2017). Proper disposal of records and equipment containing confidential and protected data for record retention to prevent the loss of documents is necessary and involves following standard operating procedures for archiving, storing, and disposing of media (Oktarina & Pramusinto, 2016).

Information technology practitioners who have the responsibility of protecting online users need to ensure strategies such as authorized users’ access to individual systems, departments, and buildings are well-defined for protecting sensitive data from any misuse of data or entry to address all critical aspects of the business (Hettiarachchi & Wickramasinghe, 2016). Other management controls focus on physical security and the environment. For example, a security guard can be present with an access list that identifies individuals allowed into a secured area.

An information security management system is a procedural security control that administratively consists of approved policies, procedures, standards, and guidelines for planning and assessment that help reduce and manage risk daily in organizations (Kalaiprasath et al., 2017; Wanyonyi, Rodrigues, Abeka, & Ogara, 2017). This security control instruct IT security leaders about how the business will be run daily and provides an ongoing review of the organization’s risk management capabilities (Kalaiprasath et al., 2017; Wanyonyi et al., 2017). Reviewing existing security policies such as data backup plans, password management policies, security updates, patch timelines, training, and other related details is a strategy that can be leveraged to conduct practical risk assessment in mitigating data breaches (Soomro et al., 2016). Some standard management controls include information security risk assessment, vulnerability assessment, penetration testing, security laws and regulations, leaders and policymakers, governance, and security threat management.

Information Security Risk Assessment

The establishment of an information security risk assessment (ISRA) begins with risk identification and assessment (Barton, Tejay, Lane, & Terrell, 2016). The ISRA is a significant part of an information security management system and a vital steering tool for IT security leaders in any organization who want to manage information security threats and to identify vulnerabilities and dangers on their network, by providing a path to decide which countermeasures can address the potential threats (Mayer et al., 2019; Shameli-Sendi et al., 2016). Risk management is a business approach expected to develop commercial environments for restricting events that may impact an organization’s assets (Soomro et al., 2016). Business risk, like IT security risk, is difficult to detect and manage. Users accessing online technology may not recognize that security threats exist while accessing the network, which may be why IT security managers should continue to apply behavioral patterns for mitigating, coping with, or avoiding such risks (Soomro et al., 2016).

A common misconception in the risk management process within an organization is separating the security system, including its risk management system, and treating it as an isolated element (Hoffmann, Kiedrowicz, & Stanik, 2016). IT security leaders face not only several types of security threats and vulnerabilities daily but also a security risk of all its IT assets (Höst, Sönnerup, Hell, & Olsson, 2018). Another challenge with security risk is that even with robust security controls in place, and following security best practice, newly discovered software vulnerabilities can render a device weak and it may quickly become exploitable (Höst et al., 2018). As a result, management in charge of ISRA should perform a rather hard triage to ensure that scarce organization resources are assigned to the risk areas with the highest priority and to protect themselves cost-effectively (Kalaiprasath et al., 2017; Mayer et al., 2019; Shameli-Sendi et al., 2016).

Leaders of organizations of varying sizes may face problems differently in selecting suitable risk assessment methods that satisfy their needs (Shameli-Sendi et al., 2016). One of the best strategies to solve information security risk problems is applying a holistic risk-based approach (Shameli-Sendi et al., 2016). Such an approach helps qualify and quantify risks within an organization so that the IT security administrators can focus on allocating resources to severe risk areas (Kalaiprasath et al., 2017; Shameli-Sendi et al., 2016).

Regular security risk assessments can help IT security leaders seal the loopholes that could create vulnerability in the network (Kalaiprasath et al., 2017; Shameli-Sendi et al., 2016). IT security leaders who do not conduct risk assessment regularly and adequately may experience severe consequences, such as loss of reputation, legal issues, or even a direct financial impact (Shameli-Sendi et al., 2016). To manage security risk effectively, IT professionals must be aware of the place and role that risk management plays in the security management process (Hoffmann et al., 2016). A security assessment will also help IT professionals to identify risky employee behavior and take actions that will better train them (Soomro et al., 2016). These techniques may provide relevant information on the complexity of data breaches, and the ISRA can assist IT security managers who have the responsibilities of finding out which organization assets are most critical to ensure adequate data protection and what data exposure can cause a significant impact to cause organizations to stop operations (Kalaiprasath et al., 2017; Mayer et al., 2019; Shameli-Sendi et al., 2016).

Vulnerability Assessments and Penetration Testing

A vulnerability assessment involves an attempt to discover vulnerabilities or flaws within a network (Ali & Awad, 2018). Vulnerability from the IT disaster management perspective means assessing security threats from potential dangers between technology users and organization infrastructure (Ali & Awad, 2018; Gangwar & Date, 2016; Ibrahim & Kant, 2018). Vulnerability assessments point to identifying the vulnerabilities or potential threats present in each organization system resource and helping to identify, quantify, and prioritize the weaknesses within the system (Ali & Awad, 2018; Gangwar & Date, 2016; Ibrahim & Kant, 2018). A process to mitigate or eliminate the most serious vulnerabilities for the most valuable resources is to investigate the risks surrounding the system using penetration testing (Alhassan et al., 2018; Ali & Awad, 2018; Goel & Mehtre, 2015).

Penetration testing, also referred to as ethical hacking, is an authorized simulated cyber-attack conducted on a network system to evaluate the security of systems (Alhassan et al., 2018; Goel & Mehtre, 2015; Ibrahim & Kant, 2018). The method involves scanning an entire network to identify all end units and vulnerabilities within the organization system (Alhassan et al., 2018; Goel & Mehtre, 2015; Ibrahim & Kant, 2018). The primary reason for performing penetration testing on systems is to check out the vulnerabilities before an attacker does and to fix them promptly (Ibrahim & Kant, 2018). Penetration testers must aim at finding the various ways attackers can gain access into the organization network for possible vulnerabilities and try to fix them before a hacker finds and uses the same loopholes (Alhassan et al., 2018; Ibrahim & Kant, 2018).

As more user-oriented applications are deployed to the web, organizational system vulnerabilities continue to be a notable problem (Ibrahim & Kant, 2018). IT administrators can identify and assess vulnerabilities using computerized vulnerability scanning tools like an SQL injection to test the criticality of the IT assets to the organization and the availability of resources (Goel & Mehtre, 2015; Ibrahim & Kant, 2018; Shameli-Sendi et al., 2016). The most noticeable challenge faced with penetration testing is that even though IT security leaders are aware of the vulnerabilities on the network, they need a penetration tester report to justify to senior management the need to budget funds to fix the vulnerabilities (Alhassan et al., 2018; Goel & Mehtre, 2015; Ibrahim & Kant, 2018). A penetration test may also attempt to compromise a system by exploiting one or more of the unpatched vulnerabilities (Goel & Mehtre, 2015; Ibrahim & Kant, 2018; Shameli-Sendi et al., 2016).

Penetration testing helps organizations to get the security design of their web pages from an attacker’s position (Alhassan et al., 2018; Goel & Mehtre, 2015; Ibrahim & Kant, 2018). It also helps organizations to meet the legal requirements for doing business (Alhassan et al., 2018; Goel & Mehtre, 2015; Ibrahim & Kant, 2018). Penetration testing is a suitable security control mechanism for testing new technology and ensuring that the technology is configured securely on the network before production (Alhassan et al., 2018; Ibrahim & Kant, 2018). IT security administrators can use these methods to create possible attack scenarios by simulating an attack on the organization network in the form of a real attacker to generate vulnerability reports (Goel & Mehtre, 2015; Ibrahim & Kant, 2018; Shameli-Sendi et al., 2016).

The report generated from penetration testing may assist security managers in verifying whether the organization network is secured (Goel & Mehtre, 2015; Ibrahim & Kant, 2018; Shameli-Sendi et al., 2016). Carrying out the test does not make an organization network more secure, but it helps to find the gaps between initial and specific implementation (Goel & Mehtre, 2015; Ibrahim & Kant, 2018; Shameli-Sendi et al., 2016). These vulnerability assessment reports might be useful to organizations as they may reveal that a system is not up-to-date with current software patches, which makes it vulnerable to some attacks (Alhassan et al., 2018; Goel & Mehtre, 2015; Ibrahim & Kant, 2018; Shameli-Sendi et al., 2016). Penetration testing helps IT security managers evaluate and test the security strength of its hardware, software, networks, and other IT systems (Arachchilage & Love, 2014). Information technology professionals who administer organization networks may need to perform confidentiality, integrity, and availability triage penetration testing to ensure scarce resources earmarked for fighting data breaches are assigned to the risk areas with the highest priority to protect users and resources effectively.

IT Security Laws and Regulations

The number of security breaches in the United States continues to increase each year, despite efforts to protect consumer data from being compromised (Lewis, Campbell, & Baskin, 2015). Leaders of the U.S. government and of other bodies around the world are focusing on safeguarding computer networks and data through laws, regulations, and industry technology initiatives (Lewis et al., 2015). As a result, government leaders have enacted information security laws and regulations to increase accountability to protect consumers and proprietary data (Lewis et al., 2015). The Sarbanes-Oxley Act, Gramm-Leach-Bliley Act, the Family Educational Rights and Privacy Act (FERPA), the Payment Card Industry Data Security Standard, and the Health Insurance Portability and Accountability Act are some of the regulatory bodies tasked with maintaining compliance with U.S. government laws and regulations (Lewis et al., 2015; Pereira et al., 2017).

Regulatory frameworks like the Health Insurance Portability and Accountability Act, the Gramm-Leach-Bliley Act, and the Sarbanes-Oxley Act were enacted to enhance the confidentiality, integrity, and availability of information (Lewis et al., 2015; Pereira et al., 2017). Negligent behavior, carelessness on the part of professionals, and lack of awareness of rules and regulations are some of the reasons data breaches still occur (Pereira et al., 2017; Shameli-Sendi et al., 2016). Frank and Wagner (2018) noted that personal data protection is an essential global discussion within the education industry as the security of data becomes critical and requires all stakeholders to become aware of and educated on the standard rules and best practices for securing data.

Vendors and third-party service providers monitoring organizational networks should follow security laws and regulations. The FERPA grants certain benefits, rights, and protections to learners concerning educational records managed by institutions (King, 2016). In developing a robust security service level agreement, vendors, contractors, service providers, and partners can be held responsible for keeping online users safe (Stahl & Karger, 2016). As a result, vendors, internet service providers, and third-party service providers should be accountable for the products and services they provide, including those affected by data breaches (Stahl & Karger, 2016). Stakeholders must implement security policies in response to new and emerging security threats and comply with U.S. laws and regulations (Kongnso, 2015). IT security leaders needs to establish a process for ensuring IT infrastructure acquired or outsourced from any IT vendors or third parties complies with reasonable security measures that complement the organization’s and international best data security procedures and policy to protect user data.

IT Security Leadership and Policymakers

Over the years, school leaders have mostly faced the challenge of promoting the use of technology and of managing and enacting policies within their school districts (Becker et al., 2017; Herold, 2017). Questions often arise concerning educational leaders’ and policymakers’ preparedness in the areas of technical proficiency and security integration to ensure the safety of online users and school data protection (Demers et al., 2017; Herold, 2017). Senior management and executives should involve and immerse themselves in the entire IT security process so that online end users can have confidence in the ability of IT practitioners to lead them successfully through critical times when there is a cyber risk (Bakar, Yaacob, Udin, Hanaysha, & Loon, 2017).

Education leaders and policymakers should place a strong emphasis on security education and awareness training programs and allocate necessary resources that will provide quality technology leadership and professional development for current and future IT professionals (Esplin, Stewart, & Thurston, 2018). IT security leaders need to create policies that outline how IT security managers can protect the organization from threats. Demers et al. (2017) highlighted the need for organizational leaders to support strategies that can identify and secure all a company’s assets by demanding a cyber-liability policy from managers and vendors for likely threats involving security incidents, loss of data, and costs incurred during a data breach.

As IT security leaders work on developing IT strategies to mitigate information security risks, senior management must ensure the effective management of security strategies (Demers et al., 2017). Business and government leaders realize that effective IT security governance requires securing the confidentiality, integrity, and availability of information assets (Esplin et al., 2018; Herold, 2017). Security leaders and policymakers need to evaluate the positive and negative impacts of technology as a measure for normal business organization activities (Mishra, 2015). Senior management and executives should involve themselves fully in the entire IT service management process so that end users can have confidence in the ability of IT security managers to lead them successfully through critical times when there is a data breach (Bakar et al., 2017).

IT Governance and Security Threat Management

The emergence of IT governance and threat management has triggered the rapid evolution of high-technology applications and the necessity of ensuring best practices across organizations (Czuprynski & Smith, 2017; Shackelford, 2016; Venkatraman, 2017). Information technology governance is a framework that not only enables organizations to manage their information resources efficiently and effectively but also helps them in achieving their enterprise objectives (Venkatraman, 2017). Information technology governance sets the tactical directions for IT security within an organization by establishing a comprehensive data governance program that will ensure that data are adequately protected and vigorously safeguarded from unauthorized access or misuse or from voluntary disclosure (Czuprynski & Smith, 2017; Shackelford, 2016). Organization IT governance allows organizations to meet IT expectations, align technology with business, and mitigate their technology risks (Venkatraman, 2017).

Stakeholders need to support the implementation of IT governance as a structure and process for achieving IT security goals that align with their business strategies (Alreemy, Chang, Walters, & Wills, 2016). Information security has become a crucial element of IT governance and an integral part of organizational management (Soomro et al., 2016). Barton et al. (2016) noted that IT security governance is a challenge for business leaders and senior management, as it involves adequate risk management, reporting, and accountability. Barton et al. (2016) also noted that the IT governance team can assist information senior management and security leaders with threat management planning processes to ensure the inclusion of desired goals and objectives for organizational security policies.

Vorakulpipat, Sirapaisan, Rattanalerdnusorn, and Savangsuk (2017) also noted that institutional information collected at any point from users should be maintained and disseminated in a manner that protects privacy and confidentiality and reduces security risks. Appropriate IT governance has become essential to organizations' online safety success as the technical security team continues to implement initiatives for information security governance (Barton et al., 2016). Information technology governance can help IT security managers optimize the effective use of IT resources, provide the right solutions, ensure best practices, and manage the risks associated with the business and maximize value (Alreemy et al., 2016). According to Mishra (2015), security governance defines the direction of information security privacy, policies, and practices within an organization. In all, funding of the IT governance process can ensure the productive and practical use of IT resources in enabling an organization to achieve its operational and information security management system goals (Mishra, 2015). Several areas of concern were researched as strategies to consider in securing a school network against data breaches and uncovering potential themes for this study.

Relationship of This Study to Previous Research

Assessing threats is not enough, especially when individuals feel unprotected and think that the potential severity of a threat is high. The present threat does not change frontline users' behavior immediately. A foundational framework for examining how organization IT security professionals react to a data breach may be beneficial to this study. Liang and Xue (2010) used the TTAT to identify the presence of covert monitoring applications in the context of antispyware. Individuals must first observe a threat before assessing coping strategies (Liang & Xue, 2009). Park, Chun, and Lee (2016) explained that internet users can cope with IT threats and accomplish system outcomes using TTAT as a coping mechanism for online safety. The TTAT framework is robust in examining user behavior as related to malicious software attacks (Young et al., 2016).

Again, research has shown that technology alone is insufficient to address critical IT security challenges (Arachchilage et al., 2016). Many discussions related to data breaches have ended with the conclusion to eliminate end users from a system to ensure network security (Arachchilage et al., 2016). When it is impossible to remove end users from within a system, some scholars argue that the best possible approach for computer security is to educate the end users on threat prevention (Dey et al., 2018; Dhakal, 2018). Ghazvini and Shukur (2016) suggested that well-designed end-user security training and education could improve organization network security (Ghazvini & Shukur, 2016). Conversely, to date, there is little work published on the human aspect of performing security checks and protecting internet users from various data breaches (Alsharnouby, Alaca, & Chiasson, 2015; Arachchilage & Love, 2014; Liang & Xue, 2009, 2010). Also, enacting online safety precautions for internet users will go a long way toward protecting online users and may be useful in understanding existing and future security threats (Tsai et al., 2016). In organizations, the protection of confidential and sensitive data alongside network devices and computer systems is critical to organizational success (Huda et al., 2017). The implementation of policies and best practices will help mitigate data breaches in institutions (Hettiarachchi & Wickramasinghe, 2016).

Also, the need to understand the school environment, and weaknesses that have plagued organization networks in previous studies, has increased. As learning becomes data intensive, school district administrators routinely gather students' data to improve systematic processes but also increase the online exposure risk and harm to students (Ho, 2017). These collected data can be misplaced, stolen, or subjected to malicious analysis that reveals identities (Ho, 2017). Security breaches in Texas constituted 6.6% of the 1,579 breaches reported in 2017, comprising 105 identity theft breaches and 2.5 million records compromised, which is more than five times the 505,088 records stolen in 2016 (Identity Theft Resource Center, 2018). The Privacy Rights Clearinghouse (2016a) also reported that at least 320 schools' security-related IT incidents investigated and reported in the media were accidental misuse by insiders and deliberate attacks by hackers. Many school districts across the United States, for instance, have had students' data or records stolen or compromised (Czuprynski & Smith, 2017). The Honeoye Falls-Lima's Central School District in New York was the subject of computer trespass, where individuals or groups of persons unlawfully accessed an administrative user account (Identity Theft Resource Center, 2018). The Argyle School District in Texas also suffered a data breach where district computer systems and sensitive personal information, including employees' W-2 information appearing to be from the district superintendent through a phishing e-mail, were compromised in 2017 (Identity Theft Resource Center, 2018). In the same year in Texas, Kountze Independent School District (ISD) was hacked and locked down, and users lost access to the shared files of all 1,300 students and employees (Teitz, 2017).

Similarly, in 2017, the Bay District Schools' website was hacked, and hackers replaced the district's home page with an anime character construing an obscene gesture and text stating "Hacked by Typical Idiot Security" (Dion, 2017). In 2016, the Midway ISD in Texas reported an unauthorized disclosure and data breach about two Midway school students charged with distributing a false report and alarm after posting a screenshot of fake documents warning families about potential violence at the school (Butts, 2016). In 2015, the Mobile County School System in Alabama experienced two denial-of-service attacks that interrupted their standardized testing program (Goran, 2017). Computer systems and networks can be insecure without applying the right IT security strategy. Incidents such as Facebook hacks, an Equifax hack, and the hacking of government agencies are noteworthy with regard to how far-reaching these threats can be (Schneier, 2018).

Protecting school or district networks from a data breach is a necessity. Although hacks and privacy leaks continue to be successful, educational agencies partnering with school districts increasingly collect and maintain large amounts of data about students to provide useful and operational educational services (Huda et al., 2017). The TTAT is a logical foundational framework for examining users' behavior related to malicious software threats (Young et al., 2016). A malicious data breach can occur when operations such as metadata spoofing attacks embedded in a typical command line are bypassed to the cloud and executed as valid instances (Elkabbany & Rasslan, 2018). A malware injection attack is one type of web-based application attacks, where hackers exploit vulnerabilities of a web-based application. Malicious codes inserted into a web-based application by attackers can instantly change the course of its usual execution (Coppolino, D'Antonio, Mazzeo, & Romano, 2017; Elkabbany & Rasslan, 2018). Hacking is one of the most common forms of a data breach, totaling 482 data breaches and exposing over 16.6 million consumer records each year (Identity Theft Resource Center, 2018). Hackers also craft malicious applications, programs, and virtual machines and inject them into targeted cloud services (Chouhan & Singh, 2016). In the cloud, hackers can initiate denial-of-service attacks by overloading the targeted cloud system with service requests so that it stops responding to any new applications, which makes the network resources unavailable to users (Chouhan & Singh, 2016).

A data breach takes place when attackers deliberately gain access to a device, they can use to hide their identity on the network to perform attacks on others (Krombholz, Hobel, Huber, & Weippl, 2015). Social engineering is another way to conduct data breaches to perform identity theft using human interactions such as social skills as an attack mechanism to obtain or compromise information about institution computer systems or networks (Gupta, Arachchilage, & Psannis, 2018). Hackers use social engineering by pretending to be genuine or a member of the team to send links to people to get them to visit a phishing page or to download malware to their system (Krombholz, et al., 2015). The Crowley ISD superintendent, through the district website, reported possible phishing scam attacks on employee W-2s and a ransomware attack where a computer was compromised, which exposed sensitive and confidential information belonging to educators, employees, students, and their families (Crowley ISD, 2018). Victoria ISD learned of a potential data security incident during the second half of 2017 in which e-mail accounts belonging to applicants and former and current employees containing personal information might have been accessed without authorization (Victoria ISD, 2018).

The resilience of IT resources from internal and external threats is critical to the success of any organization (Yalof & Chametzky, 2016). Top management and IT leaders are always searching for best practices that will minimize their exposure to security threats and reduce the cost of responding to a data breach (Blake, Francis, Johnson, Khan, & McCray, 2017; Yalof & Chametzky, 2016). A Verizon (2019) explained that threats exist where there is an incentive for malicious activity, and the education sector is one of these areas. Critical analysis of an organization' systems network activity is, therefore, a fundamental component of the early detection and mitigation of threat emanating from within. The same applies to external threats, even though the latter may come with other untold complications. Sensitive records maintained for students and parents resulting from the availability of high-speed internet connections from the one-on-one computing era to the adoption of the Internet of Things make schools targets for building botnets by hackers (Shameli-Sendi et al., 2016).

Knowledge of insider threats in information systems is essential to help address the dangers lurking within organizations (Balozian & Leidner, 2017). Intentional data leaks can occur from either external parties or malicious insiders and are typically caused by hackers' break-ins, malware, viruses, trojans, social engineering, or developers' secure coding errors (Cheng et al., 2017). Many organizational IT security professionals reported insider threat as one of the most significant risks to their enterprise network, and a malicious insider is one of the most significant security concerns that jeopardize security through data leaks or similar errors (Mozumder et al., 2017).

Most devices and types of network infrastructure exploited daily by hackers are a result of data breach insider attacks. An insider threat is a current or former staff member, contractor, or other third-party individual with legal access to an organization’s system, network, or data who abuses it for personal gains to the detriment of the organization (Elmrabit et al., 2015; Kaghazgaran & Takabi, 2015). Researchers have consistently indicated that internal users are responsible for over 50% of reported security breaches (PricewaterhouseCoopers, 2015). Information technology security managers need to continuously pay attention to protecting high-risk personal information on school laptops and mobile storage devices such as tablets, smartphones, compact disks, or thumb drives. The insider threat is considered the most challenging problem to cope with because an insider has information and capabilities not known to external malicious agents (Elmrabit et al., 2015). It has become more complex to shop for a complete insider threat solution, let alone to solve the problem efficiently. Insider attacks are often difficult to unravel and mitigate, as they are generally carried out by those supposedly trusted by the organization (Elmrabit et al., 2015; Halaseh & Alqatawna, 2016).

An insider attack reported by Florida Virtual School was the result of a student stealing personal data belonging to more than 350,000 students, parents, and teachers (Harris, 2018). Analysts at the Privacy Rights Clearinghouse (2016b) keep a record of reported and publicized data breaches of school districts. In May 2016, Chicago Public Schools asserted that identified information belonging to 4,000 students was sent to five potential vendors in violation of district policies (Privacy Rights Clearinghouse, 2016a). Analysts at the Privacy Rights Clearinghouse (2016a) also reported that confidential information related to 30,000 students from the same school district were wrongly distributed to a charter school operator for marketing purposes. Carelessness and lack of awareness account for nearly 40% of insider security incidents (Balozian & Leidner, 2017). The difficulty in handling the insider threat indicates that internal or insider threats can no longer be handled or processed as a data-driven problem, but have developed into a combination of both data and human behavior (Gamachchi & Boztas, 2017). Hence, organizations need to push the requirements for going beyond technical capabilities to understanding the unpredictable behavior of insiders.

The most common external threats to information systems are natural disasters that can occur through a connected network or physical intrusion (Hettiarachchi & Wickramasinghe, 2016). A setback with security is that even with robust security controls in place, and advancing best practice, recently discovered software vulnerabilities could make a device unstable and easily exploitable (Höst et al., 2018). Buckman, Bockstedt, Hashim, and Woutersen (2017) elucidated that a data breach occurs when a person's financial records or information are potentially put at risk for reasons of exposure. Human ignorance and carelessness are factors exploited by phishers who steal users' data by tricking or deceiving them to bypass antiphishing systems (Al-Daeef et al., 2017). According to a threat awareness survey carried out in institutions, 70% acknowledged that they do not adhere to security best practices, while 39% of respondents revealed that they were not aware of any security policies that protect end users against viruses, spam e-mails, or adware (Ramalingam et al., 2016).

Security threats affect data and data points, as well as an entire organization's reputation such that it inflicts lasting brand damage and results in the loss of business opportunities (Mishra et al., 2017). Analysts at the Privacy Rights Clearinghouse (2016b) reported 8,804 data breaches and over 11.5 million personal breaches recorded, analyzed, classified, and categorized into internal, external, and nontraceable data breaches (Holtfreter & Harrington, 2015). These flaws associated with school district network have vividly been exposed in recent years with the number of attacks on school networks increasing owing to external attacks from vulnerabilities taking an ever-changing form as hackers continue to target school networks (Hess, 2017). Texas school district data breaches have affected nearly 23,000 students within the last two years with attacks ranging from phishing, ransomware, unauthorized disclosure and breaches, and other security incidences (Privacy Rights Clearinghouse, 2016a). Data breach and unauthorized disclosure to school computers have had hackers' access personal information and files for purposes of espionage, financial, fun, grudge, or Ideology (Verizon, 2019). Following rules issued by the U.S. Department of Education, institutions under FERPA's written consent requirement can disclose education records to third parties (Cunha, 2018; Frank & Wagner, 2018; U.S. Department of Education, 2018).

Among informed data breach alerts is a phishing attack known to be a common cause of data breaches (Arachchilage et al., 2016). Phishing attacks are usually a form of web-based or online identity theft where the perpetrator redirects users to a fake website aimed at stealing sensitive information such as usernames, passwords, passphrases, online bank details, or PINs from victims (Arachchilage et al., 2016). Since 2015, five public institutions have disclosed a data breach event that potentially exposed a significant amount of student data (Demers et al., 2017). Demers et al. (2017) also noted that a hacker gained access to a database containing information on more than 80,000 students and staff. Other forms of attacks are brute force attacks where an attacker applies all possible combinations of passwords to break encrypted passwords (Khan & Goodridge, 2019).

Although a data breach can take place in the form of a system malfunction, a hidden threat may surface that results in a backdoor threat built into various programs that allows an attacker special privileges into a system (Jain & Pal, 2017). Attackers study system malfunctions and try to operate systems by going through a backdoor to exploit the feature posing a security risk (Ahmadvand, Pretschner, Ball, & Eyring, 2018). A hacker can use a technique called *pharming* to hijack an institution's website domain name by redirecting all legitimate users to a fake website where fraudulent requests are initiated (Nashwan & Alshammari, 2017). The two most common threats used to steal user information from web applications are SQL-injection and cross-site scripting (Iqbal et al., 2016).

IT security leaders need to be sensitive and vigilant when vulnerabilities abound in devices on a network that attackers can exploit. Chipp (2016) reported that six school districts (Brookesmith ISD, Brownwood ISD, Coahoma ISD, Dublin ISD, and Panther

Creek ISD) websites in Texas suffered a data breach as attackers blocked access to all ISDs' computer systems. A ransomware attack on the district servers left data encrypted and inaccessible (Chipp, 2016).

A data breach can also happen as a form of human error. Analysts at the National School Boards Association (2017) reported that data breaches can also occur as a result of honest mistakes and accidents. There have been various instances where students' personal and sensitive information was e-mailed or made available online accidentally. School records were left behind by a school administrator on a bus after a long ride home from school. Confidential and personal documents were thrown away in a dumpster instead of being shredded. The more focused IT security managers tasks with the responsibility of keeping students safe online by identifying and preventing devices from malicious attacks, prevent systems from malfunctioning, and limit human errors in a computing system, the more their families have an increased assurance of online safety at school.

Implementing strategies or approaches to secure an organization network will increase a school district's network protection against a data breach and may help mitigate the damages that a potential security breach can inflict. Security implementation can be costly and can includes fees for technical controls (monitoring tools) and nontechnical controls such as awareness training programs (Pereira et al., 2017; Shameli-Sendi et al., 2016). Online users may not recognize that cyber threats exist on the web, which is why they need to apply behavioral patterns for mitigating, coping, or avoiding such risks (Safa et al., 2015).

Threat mitigation, coping, and avoidance mechanisms may serve as one security strategy adopted to tackle network threats (Liang & Xue, 2009). Approaches to information security are generally most effective when drawn from technical, operational, administrative, and physical controls (Gatzert & Schmit, 2016). For a security system to defeat an attack, the adversary must be detected and engaged by responsive forces and neutralized (Amundrud et al., 2017). Workable strategies for defeating external attacks include information security policies, people management, network security, an active password policy, antivirus protection and software updates, physical security, audits, network security monitoring, data backup, intrusion detection, and security education training and awareness (Li et al., 2016).

Information technology security managers who have the responsibility of securing a school network need to understand how to use these strategies to mitigate risks and ensure safety precautions when hackers dist the school network to steal personal information or impersonate legitimate users (Das & Khan, 2016). One of the most reliable concepts for improving cybersecurity protection is to design layers of defense, where each layer provides the confidentiality, Integrity and Availability of data. Rezaeibagha, Win, and Susilo (2015) reinforced the importance of technical and nontechnical security techniques in IT threat and data breach mitigation.

Transition and Summary

Liang and Xue (2009) developed the TTAT on the basal premise of the cybernetic theory and on synthesized research from studies on risk analysis, health care, psychology, and information systems as a consequence of the inability of the cybernetic theory to completely represent human behavior when faced with cyber threats. The TTAT serves as a framework that helps to explain why and how individual IT users act in specific ways to avoid IT risks. Liang and Xue suggested that IT threat avoidance behavior can be represented by a cybernetic process as users attempt to widen the distance between their current security state and the undesired (unsafe) end state. Young et al. (2016) supported the validity of the TTAT. Contemporary researchers who support the cogency of the TTAT include De Guinea and Webster (2017), Collins, Jackson, Walker, O'connor, and Gardiner (2017), Shafiq, Ahmad, and Choi (2017), and Wachyudy (2018). The TTAT hinges on the assumption that users' avoidance and adoption behaviors are qualitatively different and thus posit that human beings can avoid negative stimuli and approach positive stimuli.

Also, the TTAT makes significant contributions to the literature of IT security as it clarifies the approach-avoidance distinction. The TTAT hypothesizes that avoiding a malicious threat is not equal to accepting a safeguarding measure. The TTAT includes the assumption that the avoidance and adoption behaviors are qualitatively unrelated; hence, the use of one theory in the other context may lead to inconsistent or even false findings when applied to distinct scenarios. For instance, when a threat of spyware exists, studying the adoption of antispyware may produce results inconsistent with study outcomes that focused on spyware avoidance. Also, Liang and Xue (2009) integrated a process theory view and a variance theory view of TTAT so that both process and variance research can test the validity of the framework. The TTAT affirmed that once users become aware of a threat, they set being harmed by the malicious agent as the antigoal, which is the undesired end state. If users perceive their current state is near the antigoal, they will engage in coping mechanisms to widen the discrepancy between the current state and the undesired end state. The theory has been found useful in exploring how school administrators handle cybersecurity challenges in their networks. Even though technology continues to play an essential role in the security of an organization’s physical and digital assets, humans are the weakest link in any cybersecurity defense (Al-Daeef et al., 2017). Technical controls can, and will, fail if used alone, without the input of administrative or human control. First, the mitigation of security breaches will be most effective through awareness education, contrary to the common belief that information security is the repository of the security team only. When it comes to information security, people are as important as technology, policies, procedures, and guidelines. With proper education and training, technology users can become an organization’s most reliable line of defense and its most valuable security asset. It is, however, unrealistic to expect technology users to handle the complexities and nuances of the security environment without any preparation.

Therefore, IT education and awareness are vital to organizational security. Users and information security professionals need to remember that no technical control, no matter how well-engineered and tested, can provide a completely risk-free operation, as the human component of security, with the challenges of insiders and external attacks, can be complex. This review included a discussion on the inconsistency of the definitions of cybersecurity, challenges of data breaches, risk management, IT security assessment, internal and external attacks, security strategies, and some of the problems facing school network security. Sections 2 and 3 will include discussions of the methodology and design of this research, study participants, the impact of researcher bias, the sample and population, data collection techniques, data analysis, and a presentation of the research findings.

Section 2: The Project

In Section 2, I present a comprehensive discussion of the project. The subsections include the purpose statement, role of the researcher, the participants, the research method and design, the population and sampling, ethical research, the data collection instrument and technique, the data organization technique, data analysis, reliability, and validity. The section ends with a transition and summary.

The purpose statement relates to the strategies used by IT security managers to mitigate data breaches on their school’s network. In the role of the researcher, I took into account the fact that I was the data collection instrument. In the Participants subsection, I discuss the participants as an investigator, research professional, writer, and analyst, including what made a participant qualified and suitable to participate in the research study. In the Research Method and Design subsection, I extend the nature of the study presented in Section 1 by describing and justifying the methodology and design to include at least three sources synthesized that supports the study. In the Population and Sampling subsection, I review the procedures used to select the community suitable for the sampling to ensure data saturation. The Ethical Research subsection contains research information intended to help provide justice, beneficence, and respect for persons involved in the research as participants. It was essential that each participant understand their part in the survey before giving written consent to participate data collection phase of this study and how they could withdraw from the study. In the Data Collection subsection, I provide details on data collection for the study and describe the semistructured interview process that involved using an interview guide to collect data.

Finally, I added a discussion on the study's internal and external validity, including discovering the subject through detailed contextual analysis of numerous activities and relationships.

Purpose Statement

The purpose of this qualitative multiple case study was to explore the strategies used by IT security managers to mitigate data breaches on their school’s network. The research population was IT security managers from three school districts in Texas, which is in the south-central region of the United States, with experience executing IT security strategies that protect the school network from a data beach. The findings from this study may benefit information security practice by increasing IT security practitioners’ understanding and knowledge of the multifaceted structure of cyber-attacks that may lead to more secure school networks. The implication for positive social change lies in the potential to provide a more secure and nonthreatening online experience to students and possibly offer their parents and families an increased assurance of their wards’ online safety while in school.

Role of the Researcher

In this qualitative multiple case study, I was the researcher and primary instrument. The role of a researcher in a qualitative case study is one of a role model and mentor, teacher, interpreter, advocate, evaluator, and biographer through interviews, documents, and observation (Colorafi & Evans, 2016; Katz, 2015; Ponelis, 2015). Researchers use tools as a personal lens for data collection and exploration (Fusch & Ness, 2015; Stewart, Gapp, & Harwood, 2017). In this study, I employed a qualitative multiple case study using semistructured interviews as my first approach for collecting data, in addition to reviewing available public documents on the subject. Several scholars have recognized researchers as having prominent naturalistic characteristics for acting as the human instrument of data collection (Gehman et al., 2018; Stewart et al., 2017). My central role as the researcher was to construct open-ended interview questions that would enable selected participants who met the inclusion criteria to give as much information as possible about the topic under review.

Researcher bias has considerable potential to affect the outcome of a research study and remains the most critical threat to research validity (Fusch & Ness, 2015; Glinz & Fricker, 2015; Grover, Emmitt, & Copping, 2017). The researcher's relationship as the instrument of data collection in this qualitative multiple case research, including my preferences, may have affected the truthfulness of the study. I also had no personal, academic, or institutional relationship with the participants of the study. Personal values, beliefs, and exposure to participants are some elements that may contribute to biases during data collection (Durrant, Moore, Correa, & Smith, 2016; Noble & Smith, 2015; Stewart et al., 2017). None of the participants benefitted from or bore the burden of the risks of participating in research. Fairness is about researchers treating participants with equality (Obenchain & Ives, 2015; Roulston & Shelton, 2015). It is essential for researchers to maintain a level of professionalism, trustworthiness, and credibility during the interview process (Maxwell, Lau, & Howard, 2015; O’Boyle, Banks, & Gonzalez-Mulé, 2017). I used unique identifiers to mask participant responses to protect the identities and privacy of the participants. As an IT professional with over 10 years of technical experience and an experienced substitute teacher in one of the school districts within the city limits of Houston, Texas, the potential existed for personal bias to influence the research.

I reviewed the Belmont report, which is a summary of the ethical values and guidelines for the protection of human subjects in research (U.S. Department of Health & Human Services, 1979; WaldenU, 2015a, 2015b, 2015c). An understanding of the Belmont report ensured that, as a researcher, I would respect participants, minimize the risks, maximize the benefits of the research design, and select research participants impartially. I also completed the protecting human research participants training offered by the National Institutes of Health Office of Extramural Research with Certification Number 2162597 (see Appendix A). The Belmont report is an essential document that provides researchers with a proclamation of fundamental ethics and principles to follow when conducting research associated with human subjects, as well as guidelines for resolving ethical challenges that may emerge during the conduct of research (Miracle, 2016; Vitak, Shilton, & Ashktorab, 2016). Doing this helped to ensure that I would adhere to the requirements and ethical rules of Belmont report protocols.

To encourage the receipt of accurate data from the respondents, I avoided bias by not asking leading questions during the interview session. My objective was to conduct interviews in a manner that would allow the participants to express insights on data breaches within their organization and school district. Barnes (2017) noted that questions developed should include the input of experts in the field to generate participants' subjective responses. I administered a qualitative, in-depth, semistructured interview using an interview question guide, and I endeavored to establish a professional relationship with some of the participants. Interview sessions provide researchers with a deeper understanding of the research topic and a proper relationship with participants (Grenier & Dudzinska-Przesmitzki, 2015). Researchers use interview protocols to ensure consistency and reduce unplanned problems during the interview process (Amankwaa, 2016; Birt, Scott, Cavers, Campbell, & Walter, 2016; Smith & McGannon, 2018). My interview protocol (see Appendix B) served as my guide during the interview process. In my role as the researcher, I followed the designed interview protocol to ensure I administered the interview protocol equally to all participants to ensure fairness, reliability, and dependability.

Participants

A researcher's ability to make suitable participant selections and decisions, as well as balance involvement, helps in determining the researcher's level of credibility and expertise on the knowledge demanded in research (Baillie, 2015; Lewis, 2015; Morse, 2015). The participants in this study included IT security managers from school districts in Texas with experience executing IT security strategies that protect the school network from a data breach. A participant requirement included at least 1 year of experience.

Walden University's Institutional Research Board (IRB) requires that participants engaged in a study be protected by the researcher and that the researcher adhere to the requirements and ethical rules of the Belmont report (WaldenU, 2015a, 2015b, 2015c). After gaining approval from Walden's IRB, I sent a consent form that included an introduction letter about the study to potential participants who met the inclusion criteria via publicly available e-mail addresses. The message contained a brief description of the study and its purpose, an invitation to participate, a description and confirmation of the participants' rights, the researcher's contact details, and Walden's IRB details. The participants were explicitly informed about the information in the consent form after agreeing to participate.

I developed a professional relationship with each participant and established open communication with participants to build trust and confidence. An acknowledgment e-mail was received from each of the participants' as willingness and consent to participate in the study helped strengthen a binding agreement that represents the fact that the research study posed no risk to them, their jobs, privacy, or anything that may affect them negatively. Fink and Anderson (2015) noted that researchers might face challenges with participants who may exhibit reluctance and a lack of readiness to participate in a study. To overcome such problems, researchers need to stimulate confidence and build trust in communicating with participants as an assurance of professionalism (Belanger et al., 2013; Fink & Anderson, 2015; Graneheim et al., 2017). As the researcher, I considered the values, norms, and general cultural practices of the participants to enable them to participate willingly and efficiently in the study.

To align the participants with the overarching research question, I explained the study's significance, including the IT body of knowledge available to gain from participating in the research. I sent the interview questions to the participants before the interview date, as well as the consent form and the interview letter, which provided additional information about the study. The responses collected from the participants will remain private and confidential. Building trust between the researcher and the participants is essential for establishing credibility with participants and for providing justice, beneficence, and respect for persons involved in research as participants (Friesen, Kearns, Redman, & Caplan, 2017; Miracle, 2016; Vitak et al., 2016).

Research Method and Design

The research methods commonly used by researchers are qualitative, quantitative, and mixed (McCusker & Gunaydin, 2015). The qualitative research designs commonly used are phenomenological, narrative, ethnography, grounded theory, and case study (Gergen, Josselson, & Freeman, 2015; Onwuegbuzie & Byers, 2014; Percy, Kostere, & Kostere, 2015). This study involved exploring strategies used by experienced IT security managers to mitigate a data breach. The research method and design selected were suitable for conducting in-depth research with IT security managers working to reduce data breaches within their organization.

Method

Pacho (2015) affirmed that qualitative research methods are sensitive to the social construction of meaning and depend on the interpretation and analysis of what people do and say, without making heavy use of measurement or numerical analysis. As the researcher, I used the qualitative method to understand the viewpoints and perceptions of the participants. The focus of the qualitative approach is developing an in-depth understanding of a phenomenon and focusing its meanings on the how and why of a specific issue, process, situation, scene, or set of social interactions (Boddy, 2016; Gentles, Charles, Ploeg, & McKibbon, 2015; Guetterman, 2015). The qualitative approach is frequently the preferred strategy of researchers, who employ it to make knowledge-based claims primarily on the constructivist perspectives of participants (Boddy, 2016; Gergen et al., 2015; Percy et al., 2015; Tetnowski, 2015; Wolgemuth et al., 2015). The qualitative method was a valuable tool in this study for understanding complex phenomena and answering real-world questions within the contexts of strategies used by IT security managers to mitigate data breaches.

The quantitative method includes an emphasis on a positivist inquiry of scientific methodology using experimental designs (Schwab & Syed, 2015). The quantitative research approach primarily follows the confirmatory scientific method, with a focus on hypothesis and theory testing (Antwi & Hamza, 2015; Hussein, 2015; Katz, 2015; McCusker & Gunaydin, 2015). This study did not involve exploring the scientific method but instead included a focus on understanding participants' experiences and communicating their perspectives. Even though quantitative research is reliable, researchers find it challenging when manipulating empirical variables, which makes it more complex to understand the context of a phenomenon (McCusker & Gunaydin, 2015; Noble & Smith, 2015; Percy et al., 2015; Wolgemuth et al., 2015; Yazan, 2015). The qualitative approach provides a means for researchers to investigate complex situations and explore contemporary issues within the context of examining existing events without influencing participant behaviors (Gustafsson, 2017; Nebeker, Linares-Orozco, & Crist, 2015; Yazan, 2015). Also, the aim of researchers who use the quantitative approach is to describe, predict, and verify empirical relationships in relatively controlled settings (Schwab & Syed, 2015).

The mixed-method approach represents the integration of both quantitative and qualitative empirical research in the analysis of data within a single study (Boddy, 2016). The mixed-method approach includes consequence-oriented, problem-centered, and pluralistic form of collect data to derive knowledge about the problem (Mayoh & Onwuegbuzie, 2015; McCusker & Gunaydin, 2015). How researchers collect data will depend on the nature of the inquiry and the philosophical outlook of the person conducting the research (Boddy, 2016). This study aimed to understand complex phenomena and obtain answers to real-world questions, even though the mixed-method approach includes subsequent investigations on pragmatic grounds by relying on probabilities to generalize outcomes. Also, the mixed-method approach includes investigations from both quantitative and qualitative experiments and methods within a single study in an attempt to understand the research problem (Cooperrider & Srivastva, 2017; Cronin & Lowes, 2016; Mayoh & Onwuegbuzie, 2015). Combining qualitative and survey data by quantifying the data may lead researchers to work under tight budgetary and time constraints (McCusker & Gunaydin, 2015). As I did not require extensive qualitative data analysis and multivariate analysis of quantitative data, the mixed-method approach was not suitable for this study.

Both quantitative and mixed-methods approaches were unsuitable for this study. The aim of the qualitative approach was to explore, discover, and understand the meanings embedded in the participants’ experiences through the researchers’ perceptions at understanding issues raised, provide an in-depth investigation and addresses the what, how, and why questions raised in the study (Hesse-Biber, 2016; Onwuegbuzie & Byers, 2014; Percy et al., 2015; Wolgemuth et al., 2015). This study involved exploring the strategies IT security managers used to mitigate data breaches without any intention of generalizing or experimenting with the data collected across school districts.

Research Design

The case study was the design used in this study. Researchers select a case study design to obtain in-depth information and explore contemporary issues within the context of a realistic behavioral event (Fusch & Ness, 2015; George, 2019; Harrison, Birks, Franklin, & Mills, 2017). The case study design is one of the most flexible models in research, as it encompasses a variety of accepted methods and structures that best answers the how or what of research questions (Gaya & Smith, 2016; Mayoh & Onwuegbuzie, 2015; Percy et al., 2015). The strength of a case study lies in its ability to assist researchers in exploring multiple sources of evidence, such as documents, artifacts, and interviews, without influencing appropriate behaviors (Fusch & Ness, 2015; Gustafsson, 2017; Wohlin & Aurum, 2015).

A multiple case study is a suitable research design when exploring new or emerging complex phenomena (Nebeker et al., 2015). The advantage of using a multiple case study is that a researcher can analyze data within each situation and across different locations (Gustafsson, 2017). Researchers study numerous cases to understand the similarities and differences between facts from various participants that can provide a study with a robust information (Gustafsson, 2017). Evidence generated from a qualitative multiple case study is robust and reliable, and researchers can clarify if the results from the findings are invaluable (Mohajan, 2018). Consequently, a multiple case study design was the most suitable choice for this study.

Hopkins, Regehr, and Pratt (2017) detailed that researchers conducting a study with a phenomenological design bracket their own experiences in a prolonged engagement to develop an understanding of the participants. Researchers want to understand the nature of human experiences concerning a phenomenon to gain the truth of the participants' lived experiences in their natural outlook as described by participants (Giorgi et al., 2017; Percy et al., 2015; Zeeck, 2012). Researchers choose the phenomenological design to understand the lived experiences of the participants rather than to develop patterns (Fusch & Ness, 2015; Giorgi et al., 2017; Malterud et al., 2016; Wolgemuth et al., 2015). In contrast, I sought to examine individuals' life events holistically to understand the causes. Hence, I did not consider the phenomenological design for this study.

This study did not include a narrative design. Researchers use the narrative design to weave together a sequence of events, usually from one or two individuals, to form a cohesive story generally by conducting in-depth interviews, reading documents, and looking for themes to demonstrate how the individual stories illustrate the life stimuli that created them (Harrison et al., 2017; Joyce, 2015; Wolgemuth et al., 2015). The narrative approach incorporates many such as biographies, autobiographies, and life stories, to individual accounts to make inquiries by combining views from participants' lives with those of the researchers' experience in a collaborative narrative (Percy et al., 2015).

Ethnography was also unsuitable for this study. The ethnographic design has lengthy timelines to observe and involves investigating individuals’ cultural subgroups over a prolonged period (Bamkin et al., 2016; Fusch & Ness, 2015; Hammersley, 2018). In contrast, the case study design includes a detailed exploration without needing to observe participants who have experienced the phenomenon (Joslin & Müller, 2016; Park et al., 2016). The focus of the ethnographic design is using informal methods to analyze networks of social gatherings, customs, tribes, beliefs, behaviors, and practices that define a culture (Bamkin et al., 2016; Percy et al., 2015; Yazan, 2015). The ethnographic design was not as suitable as the case study design, for exploring the truth in the participants' live experiences rather than understanding the culture of the participants.

Furthermore, I used member checking to ensure the saturation of data. Member checking is a process by which participants agree to validate answers provided during an interview and to ensure researchers capture the meaning of what participants say and that no new data are necessary (Fusch & Ness, 2015). I used the member-checking protocol in Appendix C as my guide to reestablish contact with participants. I also assumed the attainment of data saturation when new themes, information, coding, or interpretations no longer emerged from the data sources. Data saturation occurs in research when there is no further need for more data collection and analysis (Boddy, 2016; Fusch & Ness, 2015; Malterud et al., 2016; Saunders et al., 2018). According to Houghton, Casey, Shaw, and Murphy (2013), data saturation helps researchers achieve the quality and quantity of information needed as an indicator of the trustworthiness of a study. Data saturation was essential in this study to attain universal acceptance as a procedural standard.

Using triangulation to triage multiple sources of evidence in a case study helps to increase the validity of the constructs (Fusch & Ness, 2015; Wamba, Akter, Edwards, Chopin, & Gnanzou, 2015; Yazan, 2015). The study included methodological triangulation. Methodological triangulation improves the validity, credibility, and verification of outcomes in qualitative research (Joslin & Müller, 2016; Park et al., 2016).

Population and Sampling

In this study, I identified three population inclusion criteria. First, participants needed to be an IT security manager serving in one of three school districts within the state of Texas. Second, the IT security managers needed at least 1 year of experience managing security infrastructure at the organization network. Third, the IT security managers needed to be 18 years or older to participate.

Defining the Population

The population of the qualitative multiple case study met the inclusion criteria. Although some scholars avoid the number of the population sample size required as sufficient in qualitative research, because of many variabilities ranging anywhere from 5 to 50 participants as adequate (Etikan, Musa, & Alkassim, 2016; Gentles et al., 2015; Palinkas et al., 2015; Taherdoost, 2016; Valerio et al., 2016). Gentles et al. (2015) recommended that, in a qualitative multiple case study, the minimum sample size can vary between four and 10 to reach data saturation.

A minimum sample size of six participants was sufficient for this qualitative multiple case analysis and for the scale of the study based on the fundamental issue for determining population size for each school district. I reached saturation when interviewing the second participant in each school district, as the information received and collected from the first participant in each school district was not different from the information obtained from the second participant in the same school district. Samples that are too large may waste money, time, and resources, which leads to more inaccurate results (Gentles et al., 2015).

I contacted each of the participants using publicly available contact information and the inclusion criteria set for guidance and for recruiting participants of the study. The data collection strategy involved collecting interview responses from participants, transcribing the interviews, and reviewing publicly available documents to uncover patterns, themes, and rival explanations concerning the participants' strategies in mitigating data breaches on the school network. To achieve data saturation, I interviewed one participant from each school district before interviewing another participant within the same school district to determine saturation and whether the sample size would be sufficient to obtain the most reliable evidence possible. In qualitative research, a researcher uses the sample size to ensure the richness of the information, and the number of participants depends on the topic and availability of resources (Etikan et al., 2016; Fusch & Ness, 2015; Malterud et al., 2016).

Sampling

There are different strategies for sampling. The probability sampling, which is rarely appropriate when conducting qualitative research, and nonprobability sampling, which researchers use mainly in qualitative studies, are techniques for performing sampling in research (Etikan et al., 2016; Sharma, 2017). The nonprobability sampling technique is useful for pilot studies, case studies, qualitative analysis, and hypothesis construction (Etikan et al., 2016; Sharma, 2017). Nonprobability sampling techniques include purposive sampling, convenience sampling, snowball sampling, quota sampling, and self-section sampling (Etikan et al., 2016). The total population sampling which, is a type of purposive sampling technique was suitable for this study in choosing participants. The total population sampling type involves examining the entire population from a specific case that has a particular set of characteristics (Nullah, 2018; Palinkas et al., 2015). The purposive sampling technique is useful when the size of the population that has a particular set of characteristics or knowledge base is small (Etikan et al., 2016; Nullah, 2018; Palinkas et al., 2015).

The information gained from my sample represented the targeted population drawn from IT security managers engaged by one of three school districts within the state of Texas. Palinkas et al. (2015) noted that this sampling technique is suitable and widely used for qualitative case study research where researchers examine the entire population that has a particular set of attributes. Etikan et al. (2016) indicated that the sampling method enables a researcher to identify participants who will provide the needed data to answer the research questions.

I was able to select participants who understood the research subject area using the purposive sampling technique to participate in the study. I did not select other nonprobability sampling techniques, such as convenience sampling, quota sampling, snowball sampling, and self-section sampling. I did not choose the convenience sampling technique due to its limitations in allowing participants to volunteer only on the basis of their availability or accessibility rather than being accessed and invited by the researcher (Etikan et al., 2016; Malterud et al., 2016; Palinkas et al., 2015). I did not use the snowball sampling technique because it involves solely reaching out to potential participants in a chain-referral sort of system suitable for locating participants who are ordinarily challenging to reach (Etikan et al., 2016; Palinkas et al., 2015; Taherdoost, 2016; Valerio et al., 2016). I did not choose quota sampling because it includes specific criteria and several quotas set before carrying out samplings, without allowing any form of generalizations (Etikan et al., 2016; Malterud et al., 2016; Taherdoost, 2016; Valerio et al., 2016). I also did not use the self-section sampling, as the basis of the selection is the judgment of the researcher (Etikan et al., 2016; Malterud et al., 2016; Taherdoost, 2016; Valerio et al., 2016).

I did not consider the probability sampling technique for this study because it is not suitable when conducting qualitative research and included simple-random, stratified, systematic, and cluster that uses random sampling techniques to create samples (Etikan et al., 2016; Palinkas et al., 2015; Taherdoost, 2016; Valerio et al., 2016). I used the purposive sampling technique over other sampling techniques and strategies to select participants with a solid understanding of the research subject area based on their experience and knowledge. The justification for choosing the purposive sampling technique was that it helps the researcher to identify qualified participants who are willing to provide the needed data to answer the overarching research questions based on their knowledge or experience (Nullah, 2018).

Data Saturation

Oltmann (2016) noted that there is a point in qualitative research known as data saturation in which continuing to collect data only serves to confirm emerging themes. I attained data saturation when new ideas, information, coding, or interpretations no longer emerged from the data collection sources. Data saturation in qualitative research ensures researchers collect correct and adequate data using acceptable procedural standards (Fusch & Ness, 2015; Malterud et al., 2016; Saunders et al., 2018). Tran, Porcher, Falissard, and Ravaud (2016) reported that researchers using open-ended questions can conclude the analysis process at the attainment of the theoretical saturation point. For this study, I conducted individual interviews, reviewed publicly archival documents, and used a follow-up member-checking protocol to attain saturation. I reached saturation when interviewing the second participant in the same school district, as the data provided by the first participants were not different from the information obtained from the second participant.

Using multiple data sources (triangulation) enhances the credibility of studies (Neal, Neal, VanDyke, & Kornbluh, 2015). Individual interviews lessen the effect of bias during the interview process (Fusch & Ness, 2015). I used the member-checking protocol to verify the credibility of the data. Member checking further strengthens the research process. After the interview was completed, I applied a follow-up member-checking protocol to allow participants to validate my interpretations of their responses through a scheduled phone call to ensure no new data had emerged. By providing reliable data through semistructured interviews, a member-checking protocol, and a document review process, I remedied any discrepancies discovered in the data collection process. Member checking reinforced my interpretation and helped ensure accuracy.

Failing to reach data saturation may have an impact on the quality of the research conducted and hampers content reliability and validity (Fusch & Ness, 2015; Gentles et al., 2015; Saunders & Townsend, 2016). Several factors may affect a sample reaching data saturation, such as the topic of interest and study aim, the study participants, the existence of an established theory, the methods of data collection, and the methods of data analysis (Fusch & Ness, 2015; Gentles et al., 2015; Tran et al., 2016). Other challenges include researchers intruding in the participants' social settings and eliciting roles and responses that are not typical in interviews (Hussein, 2015; Oltmann, 2016; Young et al., 2018). The demanding nature of meetings, lack of trust and time, Hawthorne effects, and ambiguity of language may create obstacles (Johnsrud, 2016; O.Nyumba, Wilson, Derrick, & Mukherjee, 2018). I anticipated potential difficulties during the data collection process.

Ethical Research

According to Sugiura, Wiles, and Pope (2017), there is an increasing number of ethical guidelines and professional moral codes that guide the ethical conduct of research. However, the peculiarities of humans making the right ethical decision pose serious challenges (Johnson, Kondo, Brems, Ironside, & Eldridge, 2016). After gaining approval from Walden IRB, I e-mailed the consent form, including the interview questions and the invitation letter, to the selected participants who met the inclusion criteria. The consent form contained (a) inclusion criteria, (b) background information, (c) procedures, (d) the voluntary nature of the study, (e) the benefit of being in the study, (f) risks of being in the study, (g) privacy and confidentiality.

Informed Consent

Johnson et al. (2016) noted that research involving human subjects or participants raises unique ethical, legal, and social issues and requires informed consent. I used the consent form to inform participants about the study's aim and about their right of choice to participate, withdraw, or discontinue their participation at any point by notifying me via e-mail. Johnson et al. (2016) noted participants in research are at liberty to act according to their wishes and impulses.

Respect of Persons

Chiong, Leonard, and Chang (2017) and Grady (2018) indicated that the informed consent process should protect and respect participants' rights and dignity so that if they decide to withdraw from participating, the researcher must respect that decision. I respected the rights of the participants. Reports originating from this study will not include the personal information of individual participants. I respected the confidentiality and privacy of the participants throughout the data collection process.

Incentive

Robb, Gatting, and Wardle (2017) reported that including incentives or rewards as benefits for participating in a study could be used by researchers to encourage participants to join. I offered participants financial incentives for their involvement in the form of a thank-you gift. Participants received a summary of the findings, which they can use to learn more about some of the best strategies used by IT security managers to minimize data breaches. I also notified participants that the research might benefit future IT security managers, as written in the consent form.

Protection of Participants

I followed the Walden University IRB ethical and legal requirements guide to ensure participants were adequately protected and by ensuring no harm or risks would come to the participants as a result of being a part of this study. Fuller, Shareck, and Stanley (2017) noted that participants who are subject to low-risk participation provide more accurate research data than those exposed to high-risk study. I ensured participant confidentiality. Gergen et al. (2015) described the significance of privacy and expressed that it necessitates the protection of participants' identity in any given study.

The participants understood that the consent form served to establish a binding agreement and indicated that the research would pose no risk or harm to them. In addition, I assigned numbers and letters to each participant to ensure the participants' protection. For instance, A-P1 will represent participant 1 in school district A, and B-P3 will represent participant 3 in school district B, and C-P6 will represent participant 6 in school district C. The master key that links the codes with the participants' identities remained in a password-protected detachable device only accessible to me. Doody and Noonan (2016) encouraged researchers to use codes and encryption to protect participants' identity and ensure the protection of the data collected.

I also ensured all electronic devices, storage media, and paper documents remained secure, with electronic data remaining stored on my password-protected computer, and backed up on a password-protected hard drive. I will destroy all documents collected from participants after five years by shredding all paper documents and sanitizing the electronic media. Regenscheid et al. (2015) noted that clearing, purging, destroying, and cryptographic erasing are techniques and actions taken to sanitize electronic media.

Confidentiality

I ensured participant confidentiality and privacy by not including their names and other private information in electronic form without encrypting the electronic device. Graham, Powell, and Taylor (2015) noted that ethics in research is essential for providing confidentiality and privacy, which are participants’ fundamental human rights. I masked the identity of all volunteering participants. Lancaster (2017) recommended keeping participants’ data and maintaining them in confidence, as this contributes to the ethical trustworthiness of research and improves participants’ trust in a study. I completed the National Institutes of Health (NIH) Web-based training course "Protecting Human Research Participants" (Certification No. 2162597; see Appendix A) to enhance my knowledge of ethics-based research. I maintained sole access to all data, which will remain in a safe place for 5 years to preserve the confidentiality of the participants.

Data Collection

Data collection refers to the process of systematically gathering ideas and facts to give meaning to the descriptions and concepts of phenomena (Gaya & Smith, 2016; Hyland, 2016; Roulston & Shelton, 2015). Data have become a significant business asset in all organizations and must be protected like any other asset (Fink et al., 2017). Structured, semistructured, open, or in-depth interviews are different ways researchers can collect data (Newcomer, Hatry, & Wholey, 2015). The primary sources of data in this study were semistructured interviews and publicly available archival documents. I used the information for triangulation purposes. In the following three subsections, I discuss the data collection instruments, data collection techniques, and data organization techniques used in the data collection process.

Instruments

The researcher is the main instrument in the process of data collection (Barnham, 2015; Roulston & Shelton, 2015). In this qualitative study, I recognized my role as the primary instrument to ascertain any assumptions that may have kept me from accomplishing as many objectives as possible. In addition, I used semistructured interviews and analyzed publicly available documents on data breaches in school districts. Kallio, Pietilä, Johnson, and Kangasniemi (2016) noted that semistructured interviews allow for an in-depth exploration of the area of research by providing the researcher an opportunity to probe and expand the participants’ responses.

The semistructured interview is a viable method of collecting data in qualitative research and administered to obtain opinions of the subject and the exactness of data collected (Amankwaa, 2016; Birt et al., 2016; Smith & McGannon, 2018). Semistructured interviews are a standard instrument for data collection and a useful tool for exploring participants’ experiences, views, opinions, or beliefs on specific matters under investigation (Heale & Twycross, 2015; Lub, 2015; Palinkas et al., 2015). To establish patterns and themes, a tool to construct, design, and validate data as criteria for collecting data in a logical setting through the inductive and deductive approach will be reflected (Fusch & Ness, 2015; Stewart et al., 2017). Therefore, I conducted interviews following the interview protocol presented in Appendix B. The instrument selected using the interview protocol assisted me in narrowing down any areas of concern regarding data breach mitigation strategies.

This study included open-ended questions. Birt et al. (2016) and Kallio et al. (2016) made it clear that, during data collection, researchers should ask all participants the same questions. Adhering to the interview protocol (see Appendix B) helped me ensure I asked participants the same questions and thereby improved the reliability of my semistructured interviews. Amankwaa (2016) noted that open-ended questions should not be limited to a simple answer of true or false. The interview protocol helped me guide participants to give answers to my questions based on their previous knowledge, education, and experience relative to the topic. Qualitative data collection involves building participant trust and helping to provide insightful strategy, meanings, concepts and explanations for developing and answering research questions and outcome evaluations (Amankwaa, 2016; Kallio et al., 2016; Smith & McGannon, 2018). I also used member-checking follow-up interviews to reach the same goal.

Researchers use member checking to revalidate findings and to reaffirm participant responses (Harvey, 2015; Morse & Coulehan, 2015). Member checking permits participants to revalidate the answers and their interpretations provided during the interview (Birt et al., 2016; Harvey, 2015; Smith & McGannon, 2018). I used the responses to the open-ended interview questions as the basis for conducting the member-checking phone interviews, which enhanced the reliability and validity of the data collection instrument. Thomas (2017) noted that member checking is a research practice during which researchers offer findings as feedback to the participants to authenticate or corroborate the findings with the aim of improving reliability and building trust. Within 2 weeks of the initial telephone interview, I contacted interview participants via e-mail and followed up with a phone call to remind them of the member checking that would take place in few days to ensure the accuracy of my interpretation and the meanings of the participants' interview responses. By checking responses with participants, they are able to validate, authenticate, or refute their answers concerning researcher interpretations to the interview response provided (Birt et al., 2016; Simpson & Quigley, 2016; Thomas, 2017). Researchers use member checking as a quality control process to confirm, clarify, and augment data collected during qualitative research interviews (Simpson & Quigley, 2016).

I used available archival documents as the second instrument for triangulating purposes, in the hope they would provide insight, clarification, or support to the responses I collected in the semi-structured interviews. Fusch and Ness (2015) noted that the document review process is an adequate method for collecting the data needed to provide answers to research questions, as well as to demonstrate methodological triangulation. I reviewed publicly available school district records on data breaches, policy documents, and other documents regarding guidelines and strategies used for mitigating data breaches. I searched a broad range of databases, such as papers and newsletters, archival records, articles, and reports on the school district websites that offered strategies and information on data breaches, which included previous and recent incidents. Examining documents is an easy way to access information promptly (Johnston, 2017). Through the review of research documents, I created a database of participants' experiences with data breach mitigations techniques. I also ensured that both semistructured interviews and document analysis improve the study's validity and reliability. Using multiple data sources for methodological triangulation increases the internal validity and credibility of the research (Neal et al., 2015). I used methodological triangulation to improve the reliability and validity of my study by adding data sources such as guidelines on the responsible use of technology from the school districts, security policies, and archival documents on data breaches from other school districts. Using multiple sources of evidence, such as archival document data and interviews, allows for comparisons. Perkmann and Schildt (2015) noted that methodological triangulation with archival documents enables researchers to control any potential self-reporting and retroactive bias from the interview data. Using multiple data sources of evidence such as archival data and interviews allows for a comparison in the research, which assists researchers with data validation (Canales, 2015). Triangulation refers to using different methods or data sources in qualitative research to develop a comprehensive understanding of a phenomenon and to test for validity through the convergence of information from the various data sources (Neal et al., 2015; Perkmann & Schildt, 2015). I triangulated the responses obtained from the semi-structured interviews and reviewed publicly available school district records such as incident reports associated with a data breach, security guidelines, and policy statements that served as archival documents to increase reliability and validity. I documented all documents reviewed for triangulation purposes in a Microsoft Word document as interview data.

Data Collection Technique

The data collection technique involved using archival document review and conducting semistructured interviews. The interview process started by using a semistructured interview protocol that met the parameters set (see Appendix B). One advantage of conducting semistructured interviews is that it helps the researcher explore participants' experiences and the meanings attributed to them (Hussein, 2015; Johnsrud, 2016; Oltmann, 2016; O.Nyumba et al., 2018). Another advantage of using semistructured interviews is they allow researchers to carry out in-depth analysis from a relatively small sample that focuses on the views of participants by way of its versatility and flexibility (Kallio et al., 2016). Paine (2015) recommended that researchers ask participants the same questions to improve the reliability of interviews. I employed open-ended questions (see Appendix B) to capture the necessary data that would potentially address the research question. Clear and concise interview questions help researchers improve the reliability of responses (Ibrahim & Edgley, 2015).

After I received IRB approval, data collection commenced. Participants received an invitation letter and a consent form containing the interview questions (see Appendix B). The consent form detailed the purpose of the study, the withdrawal process, privacy, and benefits. Individuals who agreed to participate replied via e-mail with the phrase "I consent" as an acknowledgment that they understood the purpose of the study and their role as a participant in the data collection process. After the participants provided consent and shared their details, I scheduled phone interviews with them.

The qualitative interviews began with a concise introduction of myself and by clarifying the purpose of the study to the participants. I explained the consent document to the participants to ensure they understood. After the participants provided consent, I obtained permission from each participant to audio record the interview session to limit the need for me to take notes, and then I posed the open-ended questions. I recorded the interviews using a digital handheld voice-to-text recorder, and a smartphone recorder was available as a backup. Recording interviews helps researchers identify any unrecognized thoughts, feelings, and impressions that might lead to bias in research if unchecked (Neal et al., 2015; Rose, Brotherton, Owens, & Pryke, 2018). Audio-recorded interviews also help researchers code, revisit, and analyze the data by checking for emerging themes and remaining true to participants (Ibrahim & Edgley, 2015; Neal et al., 2015).

I asked probing questions to promote a more in-depth interpretation of the participants' responses. Taylor et al. (2016) noted that open-ended questions encourage discussion on the research topic, and Franke et al. (2015) indicated that probing questions illuminate a particular answer for clarification. I used rephrasing techniques to ensure I accurately captured the participants' meanings. After asking all the open-ended questions in the interview protocol, I thanked the participants for their time and assistance. I notified the participants that a follow-up member-checking process (see Appendix C) would take place approximately 2 weeks after the interview to increase the credibility, accuracy, transferability, and validity of the data collection instrument. I transcribed the records using the software transcriber Dragon NaturallySpeaking, and I replayed the audio recordings of the interviews to achieve accuracy in the data record process. Neal et al. (2015) noted audio recordings preserve verbal and nonverbal information.

However, using interviews as a data collection technique has some drawbacks. Some of the drawbacks researchers face when using interview techniques may include reduced response rates, the possibility of collecting inaccurate data, and the difficulty convincing respondents to participate in the study (Krosnick, 2018; Young et al., 2018). Another disadvantage of the interview technique is that it can be time consuming due to the need for extensive coding and can result in different interpretations because researchers may not understand and transcribe interviews in the same way (Al-Sohbani, 2016; Hashemnezhad, 2015). Using open-ended questions also has disadvantages, even though it gave me an opportunity to have in-depth discussions with participants, which improved my communications and interpersonal skills. Taylor et al. (2016) noted that researchers who ask open-ended questions can gather insights on the specific case under study. Open-ended questions are useful for obtaining ideas on changes and improvements from the respondents (Cochran, Baker, Benson, & Rhea, 2016; Taylor et al., 2016; Walther et al., 2017). Disadvantages associated with open-ended questions is they can be time consuming, and answers from different participants may be different in detail and scope (Popping, 2015).

I used member checking to ensure the flexibility and validity of data. I replayed the audio recordings to help me interpret the answers provided during the interviews and asked the participants to verify the accuracy of their responses to validate the data collected. The use of member checking helps to increase the reliability and dependability of a study (Pathak & Intratat, 2016; Thomas, 2017). Member checking took place in the form of a follow-up telephone interview (see Appendix C) within 2 weeks after the initial interview session to confirm participants' answers to all research questions. The participants clarified or commented on my interpretations of their responses to the interview questions to make sure I understood their viewpoints. After the participants agreed with the findings, I summarized each interview response for thematic analysis and developed a summary for the member checking to illustrate the themes emerging from individual responses. Harvey (2015) explained that member checking is the practice of bringing answers back to research participants for revalidation and confirmation of their initial reactions to the interview questions.

The interview included the following step-by-step process to collect data, which served as my guide in preparing for data analysis:

- I obtained approval from the Walden University IRB to proceed with the data collection process.
- Before the interviews commenced, participants acknowledged receipt of the consent form as confirmation of their understanding to participate in the study. The consent form contained the open-ended questions (see Appendix B) sent along with the invitation letter.
- I conducted interviews that each lasted approximately 60 minutes, and I used the open-ended interview questions (see Appendix B) to capture the necessary data that would be suitable for addressing the research question.

- I recorded participants’ interviews using a handheld voice-to-digital-text recorder and a smartphone recorder available as a backup to limit note taking.
- I transcribed the interviews verbatim for coding purposes using Dragon NaturallySpeaking and the NVivo software tool to reproduce the voice to text to ensure accuracy and to summarize my interpretation of the responses for validation and member checking (see Appendix C).
- After the interview, I thanked the participants for their time and assistance and notified them of a follow-up member-checking process (see Appendix C) that would take place approximately 2 weeks after the interview to increase the credibility, accuracy, transferability, and validity of the data collection instrument.
- I performed member checking with each participant via a second phone call by reviewing the responses provided by each participant during the initial interview to ensure the accuracy of my interpretation and to ensure meanings drawn from the participants’ answers were accurate.
- I imported the audio files into a Microsoft Word document for the commencement of data analysis.

Data Organization Techniques

The data collected from the interview session was recorded using a digital handheld voice-to-text recorder, and a smartphone recorder was available as a backup. According to Phillips and Lu (2018), researchers use software to assist them in organizing and keeping track of research data. After I reviewed the transcribed data for comprehensiveness, I consolidated the results into themes using QSR NVivo 12 Pro software.

Data organization tools such as NVivo help researchers organize the data collected from sampled participants (Zamawe, 2015). The QSR NVivo 12 Pro software was the central system database used to keep track of, import, organize, manage, and analyze all electronic data. After I gained permission from a participant through the signed consent form to audio record the interview, I audio recorded the interviews to reduce note taking. I used NVivo to input, organize, and store data for coding and exploring themes while maintaining the confidentiality of each research participant. NVivo supports qualitative inquiry by helping researchers organize, analyze, and find insights in qualitative data from interviews, open-ended survey responses, journal articles, documents, social media, and web content (QSR International, 2019).

I imported the transcribed textual audio-recorded interviews into a Microsoft Word document, and I uploaded the data into QSR NVivo 12 Pro for Windows. Data from the interview were organized into rows and columns using Microsoft Excel documents. I used alphanumeric codes to mask the participants' identity. I assigned each participant an identifying number ranging from 1 to 6, preceded by the letter P (for participant). The expected strategies used by IT security managers to safeguard school district networks against data breaches appeared in the columns, and the responses provided by each participant (P1–P6) filled the rows.

Data from this study do not contain the identities of individual participants. I protected the confidentiality and privacy of the participants throughout the study by using a unique identifier to code and protect their identities. The master key linking the number and alphabet codes to participant names was stored separately from the data in a password-protected detachable device only available to me. All paper documents and electronic media related to the study were encrypted and will remain in a locked storage cabinet for a period of 5 years to ensure participant protection. Researchers should encrypt, and secure all electronic media containing information on participants' identity and take action to sanitize electronic media before destroying them (Doody & Noonan, 2016; Regenscheid et al., 2015; Schmidlin et al., 2015). After 5 years, I will shred all paper documents related to the study, and I will sanitize and destroy all electronic media to protect the confidentiality of the information.

Data Analysis Technique

Data analysis is one of the critical stages undertaken in research. Many data analysis methodologies are available to qualitative researchers (Mohammad, Hassan, & Yaman, 2017). Qualitative researchers ask open-ended interview questions to collect data and explore meanings within a study (Perkmann & Schildt, 2015). I classified the data collected into different themes. Some analytical methods are domain analysis, categorical coding, keywords in context, word count, and classical content analysis (Mohammad et al., 2017).

Taylor, Dowding, and Johnson (2017) reported that researchers classify data to enhance their readability, to study the data characteristics, to strengthen data control, and to accord meaning to the data collected. I assigned different codes to identify various themes. I used a Microsoft Excel spreadsheet to maintain and store the codes, classify data themes, and analyze the data electronically. I also used the NVivo software to code and analyze the data. NVivo supports qualitative researchers by assisting them in gathering, organizing, and exploring content from interviews, document reviews, and logs to form themes (Maher, Hadfield, Hutchings, & de Eyto, 2018; Phillips & Lu, 2018; Zamawe, 2015). All data collected from the audio-recorded interviews and member-checking process, as well as secondary data obtained in the research process, were documented, characterized, and maintained based on the selected theme.

The purpose of data analysis is to uncover themes that answer the overarching research question for a study. Data analysis is an unusual step in qualitative research (Mohammad et al., 2017; Neale, 2016). Data analysis involves working through the data to discover meanings to the ideas, patterns, and descriptions that describe the research question (Zamawe, 2015). The data analysis process for this research study involved inspecting the consistency of the different data sources while employing the same method of analysis. After collecting and validating the data, I analyzed the data. Researchers use triangulation methods to carry out data analysis (Neale, 2016). Leung (2015) noted that qualitative researchers explore, describe, recognize, and make sense of patterns among words and themes to build up a significant and meaningful picture without compromising their truth, dimensionality, and richness.

According to Braganza, Akesson, and Rothwell (2017), researchers can use a wide range of techniques and strategies to achieve different types of triangulation. Data triangulation, investigators’ triangulation, theory triangulation, methodological triangulation, and philosophical triangulation are the five ways researchers may triangulate data (Braganza et al., 2017; Joslin & Müller, 2016). Philosophical triangulation was outside the scope of this study. Fusch, Fusch, and Ness (2018) noted that in data triangulation, researchers correlate data on the same event under different circumstances regarding people, time, and space. In investigators’ triangulation, researchers use more than one investigator in a study to engage in observations, interviews, coding, or analysis of participants’ responses in exploring the phenomenon (Fusch et al., 2018; Joslin & Müller, 2016). In theory triangulation, researchers provide multiple theoretical perspectives to the data set either in conducting the research or in interpreting the data (Fusch et al., 2018; Joslin & Müller, 2016).

Methodological triangulation entails two formats (within-method and between- or across-method) that use more than one option to gather data from interviews, observations, and questionnaires (Fusch et al., 2018). Researchers use the within-method format in a qualitative case study to triangulate data from multiple data collection sources (Fusch et al., 2018; Joslin & Müller, 2016; Turner, Cardinal, & Burton, 2017). In between- or across-method formats, researchers can triangulate data from a combination of quantitative and qualitative techniques in a mixed-methods study (Fusch et al., 2018; Joslin & Müller, 2016; Turner et al., 2017). In this study, I used multiple sources of data to enhance confidence and reliability in the results, and I employed within-method triangulation to analyze the data. The analysis process categorized into five steps involves compiling, disassembling, reassembling, interpreting the meaning of, and concluding the data (Castleberry & Nolen, 2018; Velte, Wilfahrt, Müller, & Steinhilper, 2017). I followed this systematic five-step process to analyze my research data.

Compile the Data

Compiling involves gathering and organizing the data that the researcher collects (Castleberry & Nolen, 2018; Velte et al., 2017). I initially created nodes and organized the data collected into these nodes relating to the coding process. I used the node categories to review the data collected, the interview records, and the archived data. I captured all reports in a Microsoft Word document removing participants' personal and identifiable data. Neal et al. (2015) emphasized the importance of using audio recordings to preserve verbal and nonverbal information. I uploaded all files from Microsoft Word into the NVivo 12 template to start the coding procedure. Braun, Clarke, Hayfield, and Terry (2019) recommended that researchers conduct a careful review of the analysis a second time to ensure data accuracy and presentation clarity.

Disassemble the Data

Disassembling entails coding the data by moving from a systematic level to a higher conceptual level of assigning codes to like words and terms (Tuapawa, 2017; Velte et al., 2017). Themes emerge from keywords and patterns when data collected are disassembled (Tuapawa, 2017; Velte et al., 2017). After the transfer and compilation of all the necessary files was complete, the next step was coding. I used the NVivo to code and simplify the data analysis process by comparing and identifying patterns. Coding involves putting together all related documents extracted from the study and study participants into basins called nodes using NVivo (Zamawe, 2015). Researchers use NVivo 12 to improve the accuracy of qualitative studies during data collation (Zamawe, 2015). Coding enables researchers to carry out data analysis and a comparison of data to extract meaningful information (Mohammad et al., 2017; Vaughn & Turner, 2016; Zamawe, 2015).

Reassemble the Data

In the reassembling stage, researchers interpret the relationships among codes, combinations of codes, and conceptually higher patterns and identify themes and patterns (Velte et al., 2017). After applying this coding process, I categorized the data set using data from the interviews and archival documents to identify unique meanings from emerging themes. I analyzed the data to extract the concepts that would directly or indirectly help me answer the research question. I also ensured the ideas that emerged from the data correlated to the conceptual framework, and the research question.

Interpret the Meaning of the Data

Vaughn and Turner (2016) noted that researchers can interpret data from interviews by coding them to ensure confidentiality and privacy. As soon as I broke down the themes, I explained the meaning of the data and made sense of it rather than repeating it. Dillaway, Lysack, and Luborsky (2017) asserted that the qualitative approach in interpreting and analyzing data involves interpreting words, not numbers. I defined and related my findings to the research question, taking into consideration that all the themes should help to answer the fundamental research question.

I examined all the data collected and classified them into codes, which later became the nodes in NVivo 12 Pro for thematic analysis. I stored the audio files, research log, and archival Word documents translated into a password-protected Excel document kept in a labeled folder. A researcher can achieve the confidentiality and anonymity of each participant by assigning generic codes to each participant (Neale, 2016; Vaughn & Turner, 2016; Velte et al., 2017). Vaughn and Turner (2016) recommended that researchers analyze data from interviews using categorical coding.

Conclude the Data Analysis

Concluding themes, ideas, and patterns derived from the overall research question is fundamental to understanding the findings of a qualitative research study (Neale, 2016; Velte et al., 2017; Zamawe, 2015). The conceptual framework is the relationship linking the literature, methodology, and results of a study (Osanloo & Grant, 2016). I analyzed the data using Liang and Xue's TATT as the framework to help me interpret the meaning of the data collected. By examining the node categories through the lens of TTAT, I compared how IT security managers can actively avoid and mitigate IT threats relevant to the phenomenon under review. I used the follow-up member-checking protocol to verify the data. Information technology users can actively avoid an IT threat when they perceive that a risk exists by adhering to security measures that will ensure their safety (Liang & Xue, 2010). I confirmed the data collected by the number of recurring themes found in the data and compared the recurring themes to previous studies to validate the results. The TTAT recognizes that IT threats exist and that individuals can apply some security measures to mitigate the threat and its associated cost as much as is feasible. Braun et al. (2019) recommended that a careful review of the analysis a second time is necessary to ensure data accuracy and presentation clarity.

Reliability and Validity

Trustworthiness is an essential feature of qualitative research, and a researcher must establish protocols for its attainment (Amankwaa, 2016; Chase, 2017; Hadi & Closs, 2016). Credibility, transferability, dependability, and confirmability are the criteria needed to validate qualitative research (Amankwaa, 2016; Leung, 2015). I used reliability and validity to indicate the degree of quality of research. I established the trustworthiness of the data using the four criteria to address dependability and by conducting a member check of my data interpretation.

I used methodological triangulation and member checking to ensure data accuracy, reliability, and integrity of the study. Triangulation helps to decrease biases and increase the validity and strength of a study (Joslin & Müller, 2016). Harvey (2015) and Chase (2017) indicated that member checking is the practice of bringing responses back to research participants for validation and confirmation of their initial answers to interview questions. Using methodological triangulation to collect multiple data sources increases the reliability, internal validity, credibility, and dependability of the research (Harvey, 2015; Morse & Coulehan, 2015; Neal et al., 2015). Methodological triangulation increases researcher confidence and allows for a comparison in the research, which will assist the researcher in validating the data (Canales, 2015). I triangulated the semistructured interviews with public school district records on data breaches, security guidelines, and policy statements as an archival document to address reliability and validity. Triangulation improves the validation and verification of outcomes of qualitative research (Joslin & Müller, 2016; Park et al., 2016).

Dependability

In qualitative research, dependability closely corresponds to the notion of reliability (Gunawan, 2015). I ensured my research interview process was transparent and logical. Researchers ensure documentation consistency and traceability to achieve the dependability of the research process (Nowell, Norris, White, & Moules, 2017; Perkmann & Schildt, 2015). I gained reliability by ensuring consistency in my study and by following the member-checking process and documenting processes during the study.

Credibility

To ensure the reliability of this study, I adhered to the research methodology, design, data collection, and data analysis. One of the techniques used to address credibility is triangulation, which researchers can operationalize through the process of member checking in a qualitative study to test the findings and interpretations with the participants (Kornbluh, 2015; Nowell et al., 2017). Participants responded to identical interview questions. I carried out the member-checking process after the interview was conducted to ensure trustworthiness. In this follow-up interview, the participants received concisely summarized answers for them to validate, authenticate, or refute concerning my interpretation of their responses to the interview questions. I examined the responses provided to the same interview questions by different participants from multiple sites. Revisiting interview responses is a way to cross-validate the answers that participants provide to the same questions (Hussein, 2015; Neal et al., 2015). I employed member checking by asking all participants to review my interpretation of their interview responses for accuracy. Member checking permits participants to verify researchers' interpretation of their responses (Birt et al., 2016; Harvey, 2015; Simpson & Quigley, 2016).

Transferability

Transferability refers to the degree of generalization or transference to which others can subject the result of qualitative research when applied in a different setting or context (Connelly, 2016). Transferability is a form of external validity in qualitative research and is an essential criterion for quality (Crandall & Sherman, 2016; Gunawan, 2015; Nowell et al., 2017). I ensured transferability by providing detailed and quality information for future researchers and readers concerning research location, participants' settings, the framework, analytical procedures, and establishing research trustworthiness. The purposive sampling technique allows a researcher to identify qualified participants who will provide the needed data to answer the research questions based on their knowledge and traits (Etikan et al., 2016; Fusch & Ness, 2015; Nullah, 2018).

A sample is a portion of a population and can also refer to the total quantity or characteristics of the things, events, or cases that are the subject of research (Amankwaa, 2016; Etikan et al., 2016; Fusch & Ness, 2015). A qualitative researcher achieves transferability when the research findings have meaning for a person not involved in the study (Connelly, 2016). Amankwaa (2016) added that researchers support the transferability of research if a study has a full description of the people studied, the context, location, transparency of the analysis, and trustworthiness of the data collected. I provide a vivid picture of the study findings and their meaning. This study may positively affect other IT security practitioners tasked with the responsibility of mitigating data breaches.

Confirmability

Confirmability is the extent to which findings are consistent, the degree of their neutrality, and the potential to be repeatable (Connelly, 2016). Confirmability puts the issue of researcher results consistent, without bias, and supported by others (Tong & Dew, 2016). As the researcher, I documented the procedures for checking and rechecking the data throughout the study. Keeping procedural memos of research logs and maintaining an audit trail of research analysis are common methodological ways of achieving research confirmability (Connelly, 2016). In this research study, I ensured confirmability by minimizing researcher bias by keeping research logs and conducting a data audit of the data collection process and analysis procedure. On researcher bias and research logs, the study remained open to new concepts that may develop from the study. I avoided the influence of cultural and personal experience while assuming the stance of a protégé who could learn from the study participants. I maintained detailed documentation and decisions as the study progressed, and I made the records available for review by a colleague.

Connelly (2016) indicated that qualitative researchers might retain and preserve detailed documentation of their study decisions and the research analysis as they move from one stage to the other. A colleague can review documentation to reduce researcher bias, broaden the research perspective, and thus improve the integrity of the research (Connelly, 2016). Audit trails are an approach proposed by many scholars in qualitative research to establish trustworthiness (Hadi & Closs, 2016). The audit trail represents an in-depth approach that helps make findings in research reflective of participants' narratives (Baillie, 2015). I provided an audit trail reflective of the research plan, strategy, and implementation of the research methodology, including the interview protocol for the data collection process, member-checking procedure, data analysis, and codes.

Data saturation is a crucial element in ensuring reliability and validity in qualitative research (Fusch & Ness, 2015). Researchers reach data saturation when there is no need for more data collection and analysis (Saunders et al., 2018). I assumed the attainment of data saturation when new themes, information, coding, or interpretations were no longer emerging from the data sources. Data saturation may have an impact on the quality of the research conducted and improves content reliability and validity (Fusch & Ness, 2015; Gentles et al., 2015). Smith and McGannon (2018) employed member checking to check for fairness and reliability. I used follow-up member-checking interview protocol (see Appendix C) guidelines and scheduled meetings with the participants to reexamine the interpretations of the collected data and to provide corroboration with or to oppose explanations and reassessments of the data analysis process. According to Houghton et al. (2013) and Kornbluh (2015), member checking is an element that contributes to the rigor of research and becomes an indicator of the trustworthiness of a study.

Transition and Summary

The increased use of technology and the internet in institutions of learning for educational purposes has made learning and record-keeping easier for institutions. The ability of IT resources to hold off internal and external threats is critical to the success of any organization (Elmrabit et al., 2015). However, like many organizations, Educational institutions are a significant target of cyber attackers. I used the TTAT and a qualitative research approach to explore the strategies that IT security managers use to mitigate data breaches in their school networks. The research participants were IT security managers from various school districts in the state of Texas who had experience executing IT security strategies that protect school networks from cyber-attacks. I analyze the collected data and present the results in Section 3. I also list the research question and discuss the research findings relative to emerging themes. Furthermore, I show how the research findings contribute to IT professional practice, make a case for the implication for social change, provide reflections, and offer recommendations for future research and action. This study contributes to IT security practice on how to reduce the number of potential cyber threats and other security incidents that students may encounter while using their school-assigned devices online.

Section 3: Application to Professional Practice and Implications for Change

The focus of this study was exploring the strategies used by IT security managers to mitigate data breaches on their school's network. In this section, I showcase findings from the data collected and analyzed, and I describe how this study might contribute to research, practice, and social change. I conclude with my reflection on the research and include recommendations for future research related to strategies for mitigating IT threats and data breaches in school district networks.

Overview of Study

This qualitative multiple case study aimed to explore strategies used by IT security managers to mitigate data breaches in their school's network. The TTAT served as the conceptual framework to capture and model observations and findings. The study population consisted of school district IT security managers in three school districts in Texas, whose roles were to manage and implement data security strategies in their institutions. Seven IT security managers agreed to participate in this study. However, I interviewed only six, consisting of two from each case. The seventh consenting participant was not available for the interview. All participants had more than one year of experience in managing security infrastructure within their network. They were all 18 years old or older. Data collection included semi-structured individual interviews (*n* = 6) and the analysis of organizational, technical, district, and public documents (*n* = 12).

Data saturation for each case occurred using the purposive sampling technique after interviewing the second participant, as I did not identify any new themes or codes when interviewing the second participants for each case. The district and public documents reviewed included a District Security Review Template, District Cyber Security Incident Response Plan, District Security Procedure, District Information Security Awareness Training program, District Data Loss Prevention Program, National Institute of Standards and Technology Cyber Security frameworks, Data Breach Response Checklist—Protecting Student Privacy, U.S. Department of Education data protection laws and regulations, and U.S. Department of Education security and privacy controls for federal information systems and organizations. Other reports included FERPA, Proofpoint, K-12 data breach report, and the Verizon Data Breach Investigation Report. Additionally, I considered the NIST cybersecurity framework policies and procedures, as referenced by participants. I used NVivo software to code interview responses, organize the coded responses into categories, and measure the frequency of words based on the number of times the words appeared in the word frequency result list. I also leveraged intercase and intracase analysis using open and axial coding and constant comparative methods to combine overlapping categories and remove redundant categories. I merged similar themes to form initial categories, and I labeled variations within categories as subcategories to identify relationships and any new emerging themes.

I used data triangulation and interviewee member checking to increase the validity of the study's findings. The inference for triangulation was to present an assembly of evidence to breed credibility (Friesen et al., 2017; O'Boyle et al., 2017; Vitak et al., 2016). Member checking of interviews took place 2 or 3 days post-interview by presenting summaries of the initial interview transcripts to each participant to review and confirm accuracy. I read each participant’s responses to him or her to ensure accuracy, credibility, and validity. Within the member-checking process, each participant was able to make changes if the interview response transcripts were incorrect and to ensure data saturation.

Presentation of the Findings

The overarching research question for this study was as follows: What strategies do IT security managers use to mitigate data breaches on their school’s network? The study involved exploring three cases. The data came from IT security manager interviews and district and public documents at three school districts within the state of Texas, whose roles were to manage, mitigate, and implement data security strategies within their school districts. Four major themes emerged from the study: frequency and risk for a data security breach, data breach safe practices and control attempts, data security implementation challenges and response setbacks, and recommendations for strengthening data breach prevention and response efforts. These four major themes, and their subthemes, relate to the discoveries found during the literature review (e.g., Czuprynski & Smith, 2017; Furnell & Vasileiou, 2017; Gamachchi & Boztas, 2017; Li et al., 2016; Pawlowski & Jung, 2015; Rezaeibagha et al., 2015; Safa et al., 2015; Selwyn & Bulfin, 2016; Tracey et al., 2017), and the outcomes from the study supported my use of the TTAT (Arachchilage et al., 2016; Boss et al., 2015; Mitra et al., 2016) as the conceptual framework used to capture and model interpretations and findings.

Table 1 includes information regarding the naming convention used to ensure appropriate isolation and suitable conveyance of information related to each theme, the participants, and the study case, leveraging the chosen conceptual framework and earlier studies to put the study findings in the context of existing literature. Three school districts were the focus of this case study. In this section, to improve the readability of the findings, the three cases have assigned identifiers (A, B, and C), representing each of the three selected ISDs in Texas. The six participants were correspondingly assigned P1, P2, P3, P4, P5, and P6. Thus, P1 represents Participant 1, P2 represents Participant 2, and so on. Two participants represent each study case. Furthermore, the nomenclature for Participants 1 and 6 in Case A has identifier A-P1 and A-P6, respectively; Participants 2 and 4 from Case B have B-P2 and B-P4, respectively, as indicators; and C-P3 and C-P5 are identifiers for Participants respectively, from Case C.

Table 1

Naming Convention for Independent School District Cases and Participants

Cases (independent school districts)	Naming convention (cases)	Participants
ISD 1	A	P1, P6
ISD 2	B	P2, P4
ISD 3	C	P3, P5

Table 2 depicts a summary of the themes that emerged from the thematic analysis of conducted semistructured interviews and reviews of organization and public documents. It highlights the categories, subcategories, and category frequencies. The four themes and their subthemes discussed in this section exemplify strategies that IT security managers in schools could use to mitigate data breaches in their institutions. I introduce, synthesize, and tie each theme to the conceptual framework and leverage earlier studies to put study findings in the context of existing literature. The discussion includes each contributing factor. The study also involved analyzing several documents. Tables 3–6 indicate the frequency of each theme in participants' interview responses and the organizational documents reviewed.

Table 2

Thematic Categories, Subthemes, and Category Frequencies

Major themes	Subthemes	Major theme frequency
Data breach—risk and frequency	Frequency of data security breaches, data security, breaches susceptibility and risk, data security compliance violation	38
Data breach safe practices and control attempts	Technical control techniques, development, and implementation of data security policies and procedures, senior management and frontline, user training, promoting online safety of students, impact reduction preparedness	81
Data breach prevention challenges and response setbacks	Lack of top management support, lack of a dedicated IT security team, response process can be time-consuming, security circumvention, lacking a solution, insufficient technical expertise, and skill set of IT security managers	44
Recommendations for strengthening data breach prevention and mitigation efforts	Implement ongoing senior management and user training programs, formulate and update policies, patch management, develop a culture of continuing capacity development and skill building for IT managers	28

Theme 1: Data Security Breach Frequency and Risk

The responses from participants supported several reports in the literature that indicated school districts are significant targets for data breach incidents, which shows that educational institutions are always at high risk for data breaches. Table 3 shows the frequency of the first major theme: data security breach—frequency and risk.

Table 3

Frequency of First Major Theme

	Participants		Document	
Major theme	Count	References	Count	References
Data security breaches—frequency and risk	6	38	5	25

A-P1 explained that schools were a prime target because they are treasure troves of valuable information. Students' information, and employees' personally identifiable information, including social security numbers and dates of birth, can be easily traded over the dark web to commit identity theft. One data breach exposed the social security numbers, home addresses, birthdates of hundreds of Texas students and their families (Martin, 2017). School districts face high costs of doing business because of data breaches. For example, the personal information from students in 39 Texas school districts was likely exposed in a data breach involving a Texas Department of Agriculture employee's laptop (Levin, 2020; Martin, 2017). Regarding the risk associated with the cost of successful data breaches, A-P1, B-P2, B-P4, and C-P5 noted that, besides financial losses to record owners, data breaches can significantly disrupt services for extended periods and incur costs associated with loss of productivity, especially if a school lacks adequate security controls so it can recover within a short period. Josey (2016) and Khan, Kim, Moore, and Mathiassen (2019) similarly asserted that the impact of security glitches puts data and systems that may be critical to business operations at a notable risk of failure and could cause an organization to lose business, suffer damage to its reputation, or close completely.

The study participants attested to the risk and damaging effects of a successful data breach based on historical evidence and training they have received. Poudyal, Dasgupta, Akhtar, and Gupta (2019) explained that successful attacks in past years in various sectors have been costly due to significant damages and business activity obstructions. A recent study by researchers at the Ponemon Institute (2019) showed that the average cost of a data breach is $141 per record in education, which may reach $200 or even higher. According to the Ponemon Institute report, the exact costs depend on the extent of a data breach, how much time it takes to identify and contain the breach, and the expenses incurred when notifying victims and resolving lawsuits. Unlike other industries, the education sector rarely experiences the hidden costs that stem from the unexpected loss of customers after a data breach (Ponemon Institute, 2019). Findings from a global study of 350 companies revealed that the average total cost of all data breaches increased from $3.5 to $3.8 million in 2016 alone (Weishäupl, Yasasin, & Schryen, 2018). The Federal Bureau of Investigation internet crime complaint center also reported that even though most of the computer attacks failed, successful breaches have cost the state of Texas over $277 million from 2010 to 2015, and Texas is consistently among the top three or four states in economic losses from cybercrime (Federal Bureau of Investigation, 2016).

All organizations or institutions with electronic records hosted or accessible on the web are vulnerable to security breaches (U.S. Department of Education, 2017). Educational institutions are the third most frequent target for cyber hackers after health care and financial services (Bolkan, 2017; Doody & Noonan, 2016; Levin, 2020).

Atapour-Abarghouei, Bonner, and McGough (2019) reported that the education sector faces the largest number of attacks per capita, with more than 10% of institutions having been targeted. Bolkan (2017) corroborated the high frequency of attacks on educational institutions and reported that the number of data breaches in the educational sector doubled in the first half of 2014. According to Levin (2020), the severity and frequency of incidents occurring in school districts are increasing. Such attacks result in billions of dollars in losses annually (Jensen, Dinger, Wright, & Thatcher, 2017; Thomas, 2018). In 2019, the K-12 Cyber Incident Map cataloged 348 publicly disclosed school incidents that included student and staff data breaches, ransomware outbreaks, phishing, and denial-of-service attacks, other social engineering scams, and a wide variety of other incidents, which was nearly three times as many incidents as publicly disclosed during 2018. The most since the K-12 Cyber Incident Map first started tracking these incidents in 2016 (Kressin, 2019).

In Louisiana, the governor declared a state of emergency in 2019 after three public school districts fell victim to ransomware, which affected 10% of Louisiana’s 5,000 network servers and more than 1,500 computers (Kressin, 2019). Ryuk ransomware struck a New York school district, where the district’s insurance company negotiated the ransom demand down to $88,000 from $176,000, which is covered (Levin, 2020; Wood, 2019). Wood (2019) noted that at Las Cruces public schools in New Mexico, a ransomware attacks infected thousands of servers and devices. The district did not pay the ransom and had to reformat nearly 30,000 devices (Wood, 2019). Levin

(2020) added that in 2019, between $600,000 and $2.9 million was lost to K-12 cybercrime in school districts in North Carolina, Oregon, and two other states.

In the State of Texas, where this study was conducted, the trend is not different. Public school systems in Texas have suffered breaches that have exposed the data of thousands of students (Bogardus Cortez, 2017). According to the Identity Theft Resource Center (2020), Texas had 105 data breaches in 2017 that resulted in the theft of 2.5 million records, which was more than five times the 505,088 records stolen in 2016. The breaches in Texas constituted 6.6% of the record number of 1,579 breaches reported nationwide (Identity Theft Resource Center, 2020). Similarly, Barden (2020) reported that Manor ISD in Texas lost $2.3 million in an e-mail phishing scam.

When speaking of factors that can motivate attackers to target an organization's data, three participants (A-P1, C-P3, and A-P6) cited espionage and sabotage. The other three participants (B-P2, B-P4, and C-P5) mentioned financial gains, students truncating upcoming exams and tests. B-P4 explained that, for quick cash, attackers will block access to information or threaten to leak sensitive information. Stakeholders and IT security leaders and may have to pay large amounts of money to protect their data, depending on the value and how rich the stolen data is. C-P3 noted that the most recent attack was for $2.4 million for a social engineering scam where hackers stole people's identity by using organizational structure to manipulate people via social engineering. The most common social engineering technique used by hackers is phishing attacks. Corporate and public documents reviewed show that more than 80% of organizations have experienced phishing attacks (Derouet, 2016). Four participants in this study affirmed that phishing e-mails are a convenient means for compliance violations that cause people to fall for phishing attacks and put the network servers at risk. Observations from the U.S. Department of Education documents reviewed further showed that hackers use phishing e-mail as a weapon to lure individuals into providing sensitive information such as financials, passwords, and other personally identifiable information. Proofpoint (2020) statistics from the document analysis showed that nearly 90% of organizations experienced targeted phishing attacks in 2019. In addition to social engineering, attackers relied on techniques such as password breaking, ransomware, and network attacks to take control of users' machine and resources that often cause further damage and disruptions (Atapour-Abarghouei et al., 2019; Poudyal et al., 2019). A 2019 report by Verizon showed that 80% of hacking-related data security breaches are due to weak, stolen, re-used, or cracked passwords. The next often used mode of attacks by cyberhackers is through malware or ransomware (Kressin, 2019). These types of cybersecurity incidents are the most expensive and disruptive, according to Kressin (2019). The relative frequency of attacks mentioned by the participants aligned with the remarks of Atapour-Abarghouei et al. (2019), who reported that the number of ransomware attacks successfully detected and prevented by most organizations increased 30% from 2015 to 2016.

According to the participants in this study, even though leaders in their institutions have assembled tools and strategies to mitigate the various network assaults from hackers, attacks have nonetheless subsided. For example, a recent report by analysts at the Texas Department of Information Resources noted that billions of attempted intrusions, which is described as malicious traffic, are blocked through its Network Security Operations Center, which shields state agencies from computer assaults (Levin, 2020; Martin, 2017). This result placed the average number of monthly malicious attempts in 2016 at 3billion (Levin, 2020; Martin, 2017). Participants in Case A and B confirmed the findings. Participants from all three cases explained that their audit logs showed a daily occurrence of continual attempts by hackers to break in. B-P2 emphasized that thousands or sometimes hundreds of thousands of blocked attempts are occurring almost daily. These affirmations are similar to comments by Kevin Gunn, director of information technology for the city of Fort Worth, who said that while the city has never sustained a major breach, a typical day in the office will see about 15,000 blocked assaults attempting to compromise the computer system (Montgomery, 2018).

Despite a large number of threats, the participants stated that successful breaches in their respective school districts were nevertheless few. All six participants had experienced non-compliance on a very small scale. Their combined assessment of the likelihood of security compliance violations occurring was less than average, ranging from 3 to 4 on a scale of 1–10. Four of the six participants interviewed felt that the likelihood of a resulting data breach was minimal. For example, on the likelihood of a data breach occurring, B-P2 said it would be like a 1% chance, and C-P5, who was from a different case study, agreed, saying, it is pretty unlikely. Both participants' perspectives aligned with a statement by A-P1, who said, so far, I have not seen anything. However, C-P3 and B-P4 had a slightly different perspective. C-P3 and B-P4 considered that the likelihood of a resulting threat depended on the characteristics of the user and the compliance procedure violated. B-P4 said, “I think it depends on where the failure is. What makes a big difference is where the failure happens.”

Like B-P4, C-P3 noted that it depends on where the threat happens. If it happens to the end-user, the likelihood is very high. Their combined assessment based on their perspective ranged from 4 to 7 on a scale of 1–10. The frequency of data security compliance violations was low, and perception about the risk that a data security compliance violation would result in an actual data breach situation varied, with most of the participants perceiving it to be significant and others perceiving it to be not significant. This theme also supports the conceptual framework to be a relevant model for phishing avoidance behavior among frontline network users in Texas. As security threat knowledge improves, individuals are more motivated to get away from the danger when they perceive the presence of an IT threat (Boss et al., 2015).

Some of the study participants revealed that, whenever a data security compliance violation and resulting data breach occurred, frontline users of the IT infrastructure were common offenders. Front-end users or employees put the institution at risk for a data security breach by (a) intentionally attempting an attack because they are disgruntled, (b) violating data security policy, or (c) ignorantly engaging with outside threats that often come in the form of phishing e-mails. One respondent from Case B recalled an incident in which an employee shared a password with an unauthorized user. Participants’ observations regarding threats from disgruntled employees support Mozumder et al. (2017), who claimed that many IT security professionals reported insider threat as one of the most significant risks to their enterprise network, and malicious insiders are one of the most significant security concerns as they jeopardize security through data leaks or similar errors. However, some of the participants expressed less concern about a data breach resulting from an internal security violation, which may be indicative of a data breach prevention strategy that may prioritize preparedness to prevent a data security breach originating from an external source over those originating internally.

These findings supported the key takeaways from the theme that, although the frequency of an actual data breach incident in the IT network of study participants is low or nonexistent, the frequency of data breach incidents in U.S. school districts, including Texas school districts (based on observations in other studies and in institutional and public records), is high and presents as an expensive problem for the data owner, the school district, and the state. The findings from the document review aligned with participants' statements that the frequency of data breach attempts is high and appears to have increased in recent years. This finding aligned with the information provided by Ho (2017) and Demers et al. (2017), who indicated that there is a relatively frequent occurrence of data security breaches in schools. Disgruntled front-end users of IT networks are often loop-holing for data breaches, as outside phishing and malware attackers are merely seeking to obtain and financially maximize the rich data and information available in education IT networks. There was a significant and widespread awareness among the participants that potential data breaches are possible and are expensive. As learning becomes more data-intensive, school district administrators routinely gather students' educational data to improve systematic processes, but this increases the online exposure risk and harm to students (Ho, 2017). Pawlowski and Jung

(2015) noted that cyber threats and other IT security threats such as data breaches had become two of the most significant risks affecting students using technology in Western societies.

Theme 2: Data Breach Safe Practices and Control Attempts

The second major theme that emerged from the analysis of the participants' responses was safe practices and control attempts for data breach mitigation. The responses from participants supported several reports in the literature, as shown in Table 4, where the frequency of this major theme was drawn. In discussing this emergent theme, five core tactical approaches relating to safe practices and control attempts that IT managers use to prevent and mitigate data security breaches in their institutions emerged as subthemes, namely (a) technical controls, (b) operational controls, (c) impact reduction preparedness, (d) senior management and user training, and (e) ensuring online safety for students.

Table 4

Frequency of Second Major Theme

	Participants		Document	
Major theme	Count	References	Count	References
Data breach safe practices and control attempts	6	81	5	117

Approach 2.1: Technical control. Putting some technical control in place was a common subtheme used by most participants to secure data on their school network. All participants revealed that they had employed technical countermeasures such as two-factor authentication, web filters, antivirus software, phishing detection software, packet monitoring software, and access lists and policies to prevent unauthorized access that

would mitigate data breaches on their school network. By leveraging the TTAT as the conceptual framework for this study, IT security professionals can establish a more effective threat mitigation mechanism in which security depends on frontline users' behavior toward avoiding the threat and on coping mechanisms. IT threats can cause severe data breach and financial losses. So, TTAT models that, when frontline users perceive that an IT threat exists, they are motivated to avoid it using coping mechanism (Arachchilage et al.., 2016; Liang & Xue, 2010).

Fink et al. (2017) indicated in the literature that many institutions use technical and non-technical security controls to monitor and reduce vulnerabilities on their network. Rezaeibagha et al. (2015) reinforced the importance of security techniques in IT security threat and data breach mitigation. By leveraging the TTAT as the conceptual framework, IT security managers can establish a more effective threat mitigation mechanism using selected technical controls and countermeasures. Information technology leaders have tested the TTAT against the context of antispyware software used to detect the presence of covert monitoring applications on a computer system (Liang & Xue, 2010; Tweneboah-Koduah & Buchanan, 2018; Young et al., 2016).

B-P2 and B-P4 reported they had a layered approach that began with the installation of a firewall and data encryption. They described it as a traditional step that everybody has had for some time. The user-access control list was necessary to access their district network resources and helped to prevent unauthorized access. B-P2 also reported having single sign-on with multifactor authentication, Office 365 Advanced Threat Protection, and data loss protection. B-P2 and B-P4 also stated they had an intrusion protection system that alerted them to log events that need further attention. B-P2 and B-P4 both acknowledged that new and existing employees undertake annual security awareness training in their institution. And that they phish test staff from time to time and recommend remediation where needed based on actions they take with the different campaigns. Mihalos, Nalmpantis, and Ovaliadis (2019) added that one of the most well-known network security mechanisms for concealing a network is using technical control. C-P3 and C-P5 added that the use of a firewall and user-access control is the most important and commonly used technical control tool for the prevention and mitigation of data breaches. C-P3 and C-P5 both agree that they also combine multifactor authentication on their network and make use of some phishing detection software like antivirus software, malware protection, encryption, monitoring, and intrusion detection systems. Bello Garba et al. (2015) reported that such security controls help to improve authentication mechanisms between an internal trusted network and an external untrusted network. Hassanzadeh et al. (2015) added that configuring technical controls provides improved protection to online users and reduces system attacks.

A-P1 and A-P6 re-emphasized the opinion of C-P3 and C-P5 by recounting that firewall, user-access control, encryption, two-factor authentication, malware protection, IDS, packet monitoring software all help to sniff out threats. They further explained that all end-user devices are configured to run on antivirus software before they can access school district networks. Mihalos et al. (2019) noted that security controls can be software, instrument, or arrangement or equipment designed to filter a network’s traffic and limit network access. Mungekar, Solanki, and Swarnalatha (2020) explained that these controls can help analyze data passing through a network and to manage and regulate traffic to and from an interface to secure appliances on a network.

All documents reviewed included recommendations for some form of technical controls. The participants indicated that technical controls, such as firewalls, were the most important and commonly used tools to prevent and mitigate data breaches. Other technical control tools mentioned included multifactor authentication, web filters that give parents the ability to monitor their children's online activities, antivirus software for all end-user devices, phishing detection software, packet monitoring software to find threats, and access lists and policies to prevent unauthorized access. This information supported the views of Kitchin and Dodge (2019), who emphasized that the purpose of adopting technical security controls is reducing surface attacks to make the exterior that is visible as robust and resilient as possible and quickly recoverable in case of failure. Aldawood and Skinner (2019) also noted that technical controls provide computerized protection from unauthorized access that supports security requirements for devices, applications, and data. Participants from all cases shared that using technical controls is a means of securing data within their network.

My analysis of organizational documents and my review of the participants' responses indicated that technical control is a critical solution used to address data breaches and can lead to a more secure online network, improved network performance, and improved user experience. Technical documents highlighted the usage of audit trails, the adoption and the use of access controls, the use of firewalls, antivirus and malware checkers, secure end-to-end encryption software, and procedures to ensure routine software patching and urgent updates to the software as they occur. Other processes include adequate offsite backups and emergency recovery plans. Technical controls contribute effectively to safeguarding data stored on network resources. IT security experts who include technical controls in their overall strategy may be able to deploy technology that will help improve the protection of staff and students online, adapt IT security policy, and apply preventive frameworks. Using technical control implementation as a tool for systems hardening will enhance the process of protecting and safeguarding personal data, securing high-risk organizational information, and condensing surface vulnerabilities (Fink et al., 2017). Participants in this study indicated that using technical control implementation as a tool for systems hardening will improve the process of protecting and safeguarding personal data, securing high-risk organizational information, and condensing surface vulnerabilities. The TTAT was valuable to this study because it demonstrates the value of IT security techniques, education, and awareness programs assisting in the mitigation of data breaches. The four most cited technical control techniques were (a) user-access control, (b) secure data communication (or encryption and authentication), (c) malware protection, and (d) IDSs.

User-access control. Evidence from the observations made by multiple researchers supports the use of user access control. This theme supports the literature when discussing the application of this technique for mitigating data security breaches. Lal et al. (2017) noted that managing user access is a technical control strategy that can help maintain a network that deters both malicious and negligent threats. DiMase et al. (2015) indicated that without authenticating and limiting user access to different network devices from multiple locations at the same time, a data breach can occur that may defile the confidentiality, integrity, and availability of data and the system. Czuprynski and Smith (2017) and Mishra et al. (2017) recommended that IT managers in organizations limit access to sensitive data only to those who need such information to fulfill their duties. In line with these recommendations, all six participants implemented a user-access control strategy to control and protect data flow and prevent data breaches in their institutions. For example, one participant (A-P1) said, “I’m very particular on who has what rights to whatever files.” Four participants (A-P6, C-P5, B-P4, and C-P3) explained that efforts to control user access typically involve using a combination of tools and techniques, including firewall, SSL decryption, two-factor authentication, access lists, security policies, zero-day detections, and guest networks for unauthorized users.

Some IT managers were more aggressive than others in terms of the number and combination of user-access techniques they implemented. For example, A-P6, B-P4, B-P2, and C-P5 separated guest networks from production networks in their districts. A-P1 and C-P4 had no guest network at all, so only authenticated personnel could access the network. A-P1 and C-P4 both agree that their network configuration is not configured to have guess networks, implying that everyone is authenticated, or access denied completely. Participants who had two separate networks had one for guests (unauthorized users) and the other for staff and students (authorized users). Networks for unauthorized users were limited to allow only necessary IT activities, such as e-mail and web browsing. B-P2 stated,

> Our guest network is for basic e-mail and web browsing, but they are physically segmented from our internal network. So, parents that come to see our students then can still have internet access without any east-west traffic within our system.

Certain aspects of the TTAT framework do not account for individual differences such as the propensity for risk, distrust, and impulsivity shown to affect cybersecurity behavior (Carpenter et al., 2019). This finding aligns and supports the conceptual framework in the aspect of the framework that indicates that individuals' perception regarding their level of susceptibility to and the resulting severity of technology threats influences their threat awareness level, which ultimately influences their motivation and behavior to avoid a threat. The Avoidance motivation of an IT security threat is the reason the TTAT applies to this study and reveals in the literature the degree to which IT frontline users are motivated to avoid IT threats by taking some safeguarding control measures proposed by IT security experts (Carpenter et al., 2019; Liang & Xue, 2010).

Lal et al. (2017) reported that an organization's network security team might authenticate user access to resources and other network applications by implementing adequate controls that restrict multiple sign-ons from one location at any given time as a strategy for mitigating a breach. In line with this observation, some of the participants remarked they also lock down their Wi-Fi to non-authenticated users, encrypt their servers, use SSL decryption to monitor packets, and install multiple layers of web filters on their servers to ensure attacks are quickly identified and blocked. One participant (A-P1) said,

> We have a web filter on our firewall, as well as another web filter that runs from the cloud with an ergonomics device. Our firewall will go out there and block all the different attacks, suspect sites for malware. We have multiple layers of filtering every data that comes in and out of our network. We are always configuring our firewall. We do not want it to accept certain traffic from specific sites and of certain quarters.

Secure data communication (encryption). Secure data communication is a second technical control technique participants used to respond to perceived threats discussed in Major Theme 1. This approach supports the literature and the conceptual framework as an approach that can be leveraged to mitigate data breaches and the TTAT to perceive the existence of a threat. Goyal (2016) indicated that encrypting data is one of the most effective ways to help keep data secured. Encrypting data helped participants control the flow of data and support the baseline configuration. The secure data communication or encryption tools that participants often cited included the use of passwords and multifactor authentication. The literature supports the main security goal of using encryption software is to secure or preserve the integrity, authenticity, confidentiality, and nonrepudiation of information (Braga & Dahab, 2015). A-P1, B-P2, C-P3, and C-P6 noted that they ensured their users reset their passwords regularly to prevent unauthorized users from intercepting the passwords or logging in to user accounts to access sensitive information. B-P4 observed the same measures whenever a password became compromised. All participants also mentioned single sign-on techniques.

***Malware protection*.** Another technical control technique that supports the literature that participants in the case study deployed for securing the school network were malware protection. According to Elkabbany and Rasslan (2018), a malware injection attack is a type of web-based application attack in which hackers exploit the vulnerabilities of a web-based application that exist due to security loopholes. Analysis of participants' responses showed that they deploy mechanisms to protect their IT systems from malicious content and to maintain data integrity. Firewalls and web filters were the most common tools participants referenced. Four of the six participants interviewed had firewalls configured to block malware attempting to enter their networks. They also regularly monitored firewall logs for unusual activity. The capability of firewalls to neutralize malicious content reduced the need for constant human monitoring. Participants also used web filters in conjunction with the firewall to screen inbound and outbound traffic.

The approach supports the conceptual framework by ensuring that front end-users are motivated to actively avoid an IT threat by taking safeguarding measures when they perceive that an IT threat exists. B-P4 and A-P6 used antivirus applications to scan removable devices automatically. Before setting up these applications, participants would test the tools for their capability to neutralize malicious content. B-P4 and A-P6 accomplished this through simulated attacks, while C-P3 and C-P5 enhanced the integrity of the software by keeping them up to date. Participant B-P4 stated,

> Penetration tests are run, kept up-to-date, while firmware and software updates are carried out monthly. To ensure a more hack-proof system locked down, I

> contract the local service and have them hit the system with plain and simple cyber-attacks and make sure that nothing is getting through.

Monitoring and intrusion detection system. An intrusion detection system (IDS) is a technical control that supports the literature, a technique supported by Thomas and Galligher (2018), and one that participants in this multiple case study employed. According to Thomas and Galligher, without proper monitoring, users may accumulate access rights that are no longer necessary and thereby increase an organization's risk of unauthorized access to data. This study showed that IT security managers used monitoring systems to detect attempted attacks and determine how frequently they occurred. Records from monitoring logs could show that attempted attacks happened daily. One participant (C-P5) said, "We do see our firewall log attack. We see daily attacks of people trying to get into our system and the mitigation activity of the firewall." Kuypers et al. (2016) noted that IT security professionals can leverage available network activity to derive risk metrics, which may lead to more informed security investments. Likewise, the participants observed that, through constant monitoring, they could tell what services were targeted. B-P2 and A-P6 noted that, in the past, monitoring systems enabled them to discover that malicious content was likely embedded in an e-mail, so there was substantial e-mail monitoring activity. A-P1, who was from the same school district as A-P6, shared a similar experience. One of the tools the IT managers used to ascertain if e-mails have had a breach was the "have you been pawned" tool. A-P1 said,

> We keep an eye on sites that will alert users on e-mail accounts that have been breached. If the tool alerts that the person's e-mail was used on a site that has a data breach, I'll have that person change their password.

One other respondent (B-P2) also had an IDS that monitored for malicious content and generated alerts that enabled the security team to initiate a response promptly. According to Venkatraman (2017), IDSs can lead to an increase in IT quality and network performance when used to identify vulnerabilities and protect the information assets of an organization from malicious attacks. They can also prevent unauthorized or inappropriate system activities from going undetected (Frank & Wagner, 2018). In explaining how the IDS helps to mitigate security breaches, B-P2 stated,

> Intrusion protection is based more on behavior. If something appears to be found abnormal inactivity, we get an alert, and we check on it, and provide remediation actions if necessary, through the advanced threat protection that has already been put in place.

This approach supports the conceptual framework by ensuring that with the right security in place, an attacker skilled at accessing a network unauthorized may be walled off by the most valuable technique in place, such that the attacker's presence can be automatically detected and kicked out of the system as quickly as possible (Tracey et al., 2017).

Approach 2.2: Development and implementation of data security policies and procedures. This approach relates to the literature by ensuring that with security best practices and security policy, IT security experts can protect end-users and organizations network against viruses, spam e-mails, and malicious online attacks. The development and implementation of data security policies and procedures strategy support Czuprynski and Smith's (2017) and Mishra et al.'s (2017) position that IT managers can employ administrative and operational controls as safe practices and control attempts for mitigating data breaches. Three participants (C-P3, B-P4, and A-P6) spoke about the presence of certain IT administrative and operational policies, and procedures inform the decision-making process and implementation of user access and password controls, as well as how they enforce IT compliance to prevent and mitigate data breaches.

Da Veiga and Martins (2015) noted that regulatory requirements are necessary to improve the information security culture in organizations such that the behavior of the workforce complies with information security and related information processing policies. The user-access policies in the school districts stipulated and encouraged the enforcement of data access rights granted to users of their IT infrastructure. Respondents leveraged these policies to ensure users could not access administrative accounts, and users were only granted access to data that was necessary to perform their duties. A certain level of authentication was necessary before anyone could access student data. B-P4 stated,

> We have an access policy . . . that nobody can access student data without showing authentic identification and signing paperwork in our front office. This process implies that no one, for example, will receive student information over the phone, by fax or e-mail, and so forth.

Participants had password policies that governed the implementation of identification and authentication controls. Their password policies stipulated that users must frequently reset passwords to prevent unauthorized users from intercepting passwords, logging into accounts, and accessing sensitive information. The same measures were in place when passwords became compromised. A-P1 said, “We have policies like changing admin credentials and things like that so that it helps prevent someone from monitoring us, log in remotely, intercept or to steal data.”

Another aspect of developing and implementing the data security policies and procedures discussed was the administrative approach employed to enforce IT security compliance. Enforcing compliance was an essential aspect of the IT managers’ data breach prevention efforts and hence included punitive measures to discourage users from going against security policy within the institutions. A-P6, for example, said,

> Any case of security compliance violation is handled promptly and accurately. The teacher who shared her password with a student got terminated, and her IP [Internet Protocol] was deactivated. The account password was changed immediately. Such measures ensure that other people understand the gravity of their actions.

The approach supports the conceptual framework by ensuring that when IT security managers believe that a threat exists and that users are aware of a safeguarding measure, the more likely to think that they can avoid the threat. The administrative and operational control techniques highlighted by participants were similar to those in the findings of Soomro et al.’s (2016) study, which suggested that IT leaders can leverage reviewing existing security policies such as data backup plans, password management policies, security updates, patch timelines, training, and other related details to conduct a practical risk assessment to mitigate data breaches.

Approach 2.3: Senior management and frontline user training. This approach 2.3 relates to the literature by ensuring that senior management involvement in deploying security strategy and a designed information security training program is necessary to enhance users' knowledge leading to improved online safety. Senior management and frontline user training are another primary data breach prevention and mitigation strategy that emerged. Well-defined information security training is necessary to enhance users' knowledge, which may lead to improved user behavior in the training process (Czuprynski & Smith, 2017; Furnell & Vasileiou, 2017; Safa et al., 2015). Most IT security experts agree that humans are the weakest link in defense of information integrity within an organization (Czuprynski & Smith, 2017; Ramalingam et al., 2016; Soomro et al., 2016). Responses from participants in the case study also indicated that the IT managers have views that are similar to those of Palinkas et al. (2015) and Ramalingam et al. (2016), who found that users' ignorance and negligence of information security practices, lack of awareness programs, and lack of training are some of the fundamental causes of data breaches. Users accessing online technology may not recognize that security threats exist while accessing the network, and this may be why IT security managers should continue to apply behavioral patterns for mitigating, coping with, or avoiding such risks (Soomro et al., 2016). Online security awareness training, workshops, security awareness posters, newsletters on security, and meetings are among the different ways IT security managers and leaders can improve users' knowledge of information security (Dhakal, 2018; Safa et al., 2015). All six participants implemented some sort of training and awareness program to generate intervention aimed at not only preventing data breach occurrences but also reducing the impact of a breach if it occurred. Participants also applied this strategy to garner top management support. To fully engage and get the buy-in of senior management, security managers in this study had to sensitize them to the need for data protection measures and remind them of their roles and responsibilities. One respondent recalled how the management had been against rolling out simulated attacks. It took the IT security team time to create awareness, after which management understood the use and the need for the exercises and approved them. As B-P2 noted,

> The phish testing was not necessarily popular in the beginning . . . but as we began to explain . . . you do a tornado drill or active shooter drill, and the reason you do that is to be prepared for the real thing. Everyone began to realize the proposed exercise was for a benefit.

Participants deployed training to prevent data security compliance violations. A-P6 explained that users' level of awareness on security requirements, roles and responsibilities, and level of compliance determined their activities. As A-P6 said, "automation systems design and architecture will always fail if the end-user or the human element is not addressed, and education is provided because that is your biggest risk."

The second participant from the same school district attributed the high level of IT security compliance to the ongoing and frequent training they carry out. A-P1 noted,

> We try and educate our users to keep that [system compromise] from happening. I have been here for eight years, and we have not had it happen yet. I think that because we educate our users on their e-mails and those sorts of things, I feel like that is why we have not had that happen.

The approach 2.3 also supports the conceptual framework by ensuring that with senior management buy-in and deploying a well-designed information security training program as a safeguarding measure, front end users can perceive at a given time the existence of a threat online and try to avoid the threat. Demers et al. (2017) indicated that for IT experts to work on developing effective IT strategies that will mitigate information security risk, senior management must ensure effective management of security strategies is in place.

Approach 2.4: Promoting online safety for students. This approach relates to the literature by ensuring that IT security managers continue to promote student online safety. One of the most reliable concepts proposed by Conteh and Schmick (2016) on cybersecurity protection is to design layers of defense. The method referred to by the participants for promoting online safety for students was the content-filtering technique, which participants used to protect students from potentially harmful content. A reason for the popularity of content filters was that because the institutions are schools and students are often targets for online bullying, which could potentially lead to suicide or murder, the risk for potentially harmful content passing through into their network is high and that the procedure for its implementation is relatively easy. Content-filtering techniques serve to protect students from such potentially harmful content, including information on suicide and murder. Multiple types of software are available for filtering contents going through a network, but the three most frequently cited software programs were Go Guardian, the beacon, and DyKnow. C-P3 and B-P4 employed the Go Guardian and DyKnow, which can flag restricted content. C-P3 said,

> We use Go Guardian . . . a web-based URL content-filtering software that we use in conjunction with our firewall for the students. So, it monitors their web traffic. Hence, by typing in the URL on the address or search bar, we capture the entered data, and it gets flagged for whatever we add . . . terms like . . . suicide . . . guns, gambling . . . adult content, etc.

Another tool referenced by C-P3 was the beacon, which flags potentially damaging information and sends alerts to security managers, enabling them to take timely actions. C-P3 explained,

> I added a feature called a beacon. It's a suicide detection and prevention tool. It flags on self-harm, suicide planning, suicide research, and things like that, and it sends an alert to the administrators. It can also be set to auto-notify the parents.

Participants protected student data by ensuring users provided a certain level of authentication, as stipulated in the user-access policy. B-P4 noted that there is a user-access policy that specifies, for example, that no student data can be retrieved by phone, fax, or e-mail without providing proper identification and signing some paperwork in the front office.

Approach 2.3 also supports the conceptual framework by guaranteeing that if users believe that the perceived online threat cannot be entirely evaded by taking the proposed safeguarding measures, they will engage in emotion-focused coping mechanisms to circumvent the threat. Other techniques referenced by the participants included parent sensitization and involvement. Three respondents, one from each of the three cases (B-P2, C-P5, and A-P6), noted they held sensitization meetings with the parents to make them aware of the security policy and their role in enhancing student privacy and security. In addition to these meetings, parents could access IT security information from social media and the school's website. This measure aligns with recommendations by Dey et al. (2018) that IT managers can enforce and design security training and sensitization in ways that attract users' attention to enhance awareness and help them retain acquired knowledge for a longer time.

Approach 2.5: Impact reduction preparedness. Recovery planning, backup systems, and senior management and frontline user training were three techniques that participants employed to reduce the impact of a data breach incident. In terms of recovery planning, one respondent believed it was essential to have well-documented recovery plans detailing the procedure for data recovery in case of a data breach. This respondent, C-P3, said,

> Have a plan in place . . . even if you don't have a complete plan, if you have a plan, where you know what to do when X, Y, or Z happens and how to respond to that, that is what's important.

In support of the literature, data breaches and cyber threats can be reduced or prevented by creating backup volumes when privileges come under threat and so that corrupted data can be recovered from the backup disk (Subedi et al., 2017). To avoid data loss and sustain business continuity, some of the IT security managers interviewed ensured proper backup policies were in place and implemented precisely. According to C-P5, “One of the most important things for us is to have an outside back up. That way, if it does happen and our data is compromised, we have an outside backup that a hacker can’t get to.” Another participant from a different school district shared something similar, saying, “Last time before we got hit. It was ransomware. . . .”. It only affected one person and one person’s network folders. So, we recovered and backed up and ran in less than two hours.”

In addition to backup policies, participants also deployed specific backup techniques. One backup procedure mentioned was encrypting data to control the flow of data from unauthorized users and baseline configurations. For example, C-P3 said, “It’s important to have a baseline and know what data you have towards your configurations for your network equipment, knowing where your backups are going to, or coming from and that those are secured.”

The backup policy strategies and techniques deployed to align with the aspects of the conceptual framework posit that if the threat cycle continues from the point where the user perceives that the current threat state is close to the set state of being harmed, the user will engage in coping mechanisms intended to expand the diminishing discrepancy between the threat state and the set state of being hurt. The backup response may indicate that the implementation of backup systems is a coping mechanism aimed at diminishing the damage that might arise from a breach.

Theme 3: Data Breach Prevention Challenges and Response Setbacks

The third major theme that emerged from the analysis of participants' responses was data breach prevention challenges and response setbacks. All respondents concluded that there are three prevention challenges:

1. Lack of top management support
2. Lack of a dedicated IT security team
3. The need to keep informed continuously on new tools that could circumvent security measures

The theme supports the literature by confirming that a lack of top management support will likely stems from high-level managers not knowing what IT managers' needs are, which could result in funding being allocated elsewhere. The lack of a dedicated IT security team will also stem from members of IT security teams having many responsibilities. However, according to the participants, technology changes so rapidly that IT security managers struggle with knowing about all the emerging tools that can bypass the security measures when implemented even though they apply automation mechanisms whenever possible.

The respondents also indicated response setbacks are additional roadblocks to their security measures. Three main response setbacks emerged as posing the most difficulty:

1. The response process can be time-consuming
2. Solutions can be lacking
3. Insufficient technical expertise and skillsets among IT security managers

Although much about IT is automated and quick, responding to breaches can take a long time. The response time is longer when IT professionals do not immediately have a solution to the problem. The participants agree that they sometimes seek expert advice from other IT professionals to help them solve issues thoroughly and expediently. While seeking advice from other IT professionals is laudable, it is further evidence that some IT security managers lack the expertise needed to solve problems on their own. What follows is an exploration into each of the data breach prevention challenges and response setbacks according to the participants in each case study, as well as potential remediation recommendations and areas for further research. Table 5 shows the frequency of Major Theme 3.

Table 5

Frequency of Third Major Theme

	Participants		Document	
Major theme	Count	References	Count	References
Data breach prevention challenges and response setbacks	6	44	5	18

The following discussion will include information on each of the data breach prevention challenges and response setbacks described by the participants in each case study, as well as provide potential remediation recommendations and areas for further study. I achieved methodological triangulation by reviewing the organizational and public documents that supported the subthemes. The referenced documents also addressed standards for data breach preventive challenges and setbacks. Analysis of the documents and participants' responses showed that the data breach prevention challenges and delayed response time from IT security managers is a complex and serious problem.

Identifying and closing all sensitive data is neither possible as a way out nor a wise goal to pursue. Moreover, with a more focused goal applied in preventing the most damaging data leaks and establishing better ways for online users to exchange information securely, data breach prevention can become active, practical, and successful. While response time can be critical, focusing first on the most significant and highest impact areas makes it easier to respond to a data breach and easier to provide a logical solution to stop the data leaks.

As some school district leaders search for ways to improve students’ data privacy and K-12 cybersecurity resilience, others are using the NIST framework to guide new regulations and guidelines. As a district IT leader, it is a good idea to be familiar with the NIST cybersecurity framework to develop, audit, and strengthen the cybersecurity infrastructure to support the fight against a data breach. The lack of a committed IT security team, and the unavailability of critical security prevention tools could circumvent data security measures. Internet content is often used to propagate malware and cyber threats. Internet content filtering can help to prevent the infection and spread of malware through internet content, even though the right tool to solutions for data loss prevention is still evolving, with no single tool providing all capabilities. Most organizations require a modular architecture that allows institutions to address their most critical requirements cost-effectively and quickly while being able to add new security controls as their needs change. Such architecture also ensures quick deployment, protects assets, and quickly scales to accommodate expansion and growth.

Prevention Challenge 1: Lack of top management support. Most of the respondents felt that they did not receive adequate support from their top management in terms of funding and supporting training programs. C-P3 said,

> The people above us don’t often realize what they need to help prevent it and do not authorize the funding for us to get whatever software that is required to help us prevent all these breaches . . . because we need to prevent it in the future in case something really huge happens.”

According to all the participants, it is challenging to build the necessary infrastructure to prevent data breaches without funds. In support of the literature, Noguerol and Branch (2018) found that institution leadership do not fully understand IT security mechanisms and are less likely to put in place measures to increase the reliability of data at risk. Demers et al. (2017) highlighted the need for organizational leaders to support strategies that can identify and secure all company’s assets by demanding a cyber-liability policy from managers and vendors for likely threats involving security incidence, loss of data, and costs incurred during a data breach.

According to B-P4, “The infrastructure is chronically inadequate, making the institution highly vulnerable to data breaches.” This statement aligns with findings by Tracey et al. (2017), noting that leaders need to be able to adopt and promote preparedness strategies by creating awareness and communicating information correctly and provide human resources, physical support, and social capital. Barton et al. (2016) noted that an IT governance team can assist senior management and security leaders with threat management planning processes to ensure the inclusion of desired goals and objectives for organizational security policies. Thus, IT security leaders must have the support of their community, institution, and management. The respondents in this study felt that they did not receive adequate support from the top management in terms of funding and support for training programs.

The approach supports the conceptual framework by ensuring that a safeguarding measure is in place in case users perceive the existence of an online threat. Institutions leadership should, therefore, place a strong emphasis on security education and awareness training program and allocate the necessary resources to provide and promote quality technology leadership and professional development for current and future IT professionals (Esplin et al., 2018).

Prevention Challenge 2: Lack of a dedicated IT security team. According to the participants' responses, a lack of a dedicated IT security team was a critical challenge. Cybersecurity talents are hard to raise and retain for every company, but it is more difficult for some than for others (Barton, 2019). Like in many organizations, dedicated security professionals are employed and equipped to implement safeguards to protect sensitive data (Plachkinova & Maurer, 2019). B-P2 said, "Being a school district, we do more than one thing. . . . For us, automation is key because we don't have second or third shift work; we have other needs that we are attending to." Buchler et al. (2018) demonstrated that a strong association existed between team functional role specialization and successful performance in cyber-defense. The amount of knowledge needed about security is relatively large.

B-P4 said, “Being a school district, we don’t have a type of security group. . . . Despite this, some teams comprise of various IT security specialists having more than one role.” P-A1 posited, “To cope with this challenge, we automate most of the security functions. This enabled us to find time to dedicate attention to other roles.” The fundamental problem facing the data security skills gap, however, is that there are not enough people entering the field (De Zan, 2019). According to the results of a survey taken by college IT and security staff to develop a better understanding of their security position, a dedicated team was lacking, which indicated that senior leaders are not taking the issue seriously (Chapman, 2019). Also, this theme supports the literature that because of lack of a technical skillset and the lack of dedication, some IT security teams manage and monitor security tools without a sound knowledge background (Barton, 2019; De Zan, 2019; He, Kshirsagar, Nwala, & Li, 2019). Lacking a skilled cybersecurity team is doing more than putting companies at risk, and it is affecting the job satisfaction of existing staff (Barton, 2019; De Zan, 2019; He et al., 2019).

The approach supports the conceptual framework by ensuring that IT security managers understand human behavior under IT threats. Cybersecurity starts and ends with educating both users and IT security professionals. Enough interest does not exist at the district level to support effective cybersecurity programs (De Zan, 2019; He et al., 2019).

Prevention Challenge 3: Security circumvention. According to the participants in different school districts, online users, especially students, often invent tools to circumvent the filtering tools that are put in place to prevent data breaches. This approach supports the literature that IT security managers had to find ways to keep up with these security circumvention activities to restrict access to blocked content. A-P1, A-P6, B-P2, and B-P4 stated that technology-savvy students attempt to hack into the school network to access restricted sites. A-P6 added, “Our major setback was the predominant use, some sort of tumbling protocol. It was a free VPN [virtual private network] client.” With increasing numbers of covert channels and steganography tools available, malicious insiders make data breaches challenging to detect (Cheng et al., 2017). Patel (2020) showed that a single firewall no longer provides the reliability and efficiency to network data needed to protect organizational networks.

Solutions for data breach prevention are still evolving, with no single option providing all capabilities required in most organizations. As more covert channels and steganography tools become available, malicious insiders make data breaches particularly challenging to detect (Cheng et al., 2017). Gamachchi and Boztas (2017) noted that, in academic settings, handling insider threat is difficult. Researchers have consistently indicated that internal users are responsible for over 50% of reported security breaches (Cheng et al., 2017).

The approach supports the conceptual framework by ensuring that users can circumvent online threats when they perceive the existence of a threat by using the effectiveness of the safeguarding measure, the costs of the measure, and the user's self-efficacy of employing the measure. Company leadership needs to design a flexible architecture that will ensure speedy deployment, that protects investments, and that quickly scales to accommodate expansion and growth to cost-effectively address their most urgent security requirements while being able to add new security controls as their needs change (Aldawood & Skinner, 2019; Bernstrøm, Drange, & Mamelund, 2019; Raja, 2019).

Response Setback 1: Response process can be time consuming. The conceptual framework describes the processes and factors of susceptibility response and self-efficacy that are negatively affected by the cost of response and how IT users engage in threat avoidance behaviors (Hewitt et al., 2017; Liang & Xue, 2010). IT experts in organizations should develop a conventional continuity plan or suite of detailed incident response plans for restoring critical business functions and applications promptly (Tracey et al., 2017). B-P2 explained that, although many aspects concerning IT are automated and quick, responding to an IT threat can take a long time. B-P4 stated, “The biggest setback we’ve encountered will be related to time. We’ve had alerts in certain areas that take time to track down where they originated from, especially if it’s in the district.” Response time is longer when IT professionals do not immediately have a solution to the emerging problem. According to Kongnso (2015), leaders in industries and institutions must implement security policies in response to new and emerging security threats and comply with U.S. government laws and regulations.

One respondent, C-P5, stated. “The biggest setback to be encountered will be related to time.” Accuracy and response time are the two essential quality concerns for an organization’s systems to be free of security threats (Babar & Ullah, 2019). Tracey et al. (2017) supported the literature that indicated an accepted conventional suite of detailed incident response plans should be developed for restoring critical business functions and applications promptly. C-P3 explained that responding to attempted data breaches can take several hours, days, or months, which disrupts services and results in a loss of productivity. Though the participants reported implementing automation mechanisms whenever possible, technology changes so rapidly that they struggle with learning about all the emerging tools that can bypass the security measures they apply. IT leaders in institutions may establish and document an incident response plan that centrally tackles all security incidents (Tracey et al., 2017). Babar and Ullah (2019) affirmed that response process time helps measure how quickly a system collects and analyzes security event data to generate alerts, which are then used to prevent an attack. Finally, IT leaders and security managers must be able to communicate response guidelines when there is a data breach (Kalaiprasath et al., 2017; Wanyonyi et al., 2017).

Response Setback 2: Lacking a solution. Participants shared that, as security managers, they do not always have a solution to every security problem that arises. During such instances, they seek expert advice, which supports the construction of the TTAT that explains users' technology threat motivations and behaviors. The conceptual framework recommends that experts seek guidance and safeguarding measures to help them solve issues thoroughly and expediently in understanding individual threat avoidance motivation and behavior as a critical component in designing effective cybersecurity solutions for both frontline users and organizations. While seeking advice from other IT professionals is laudable, it is further evidence that some IT security managers lack the expertise needed to solve problems on their own. As B-4 described,

> If I don’t know the answer, then I have people that I contract to call upon to help me get the knowledge I need and with proper reporting, get the drill down to the actual problem, and then fix it.

In this regard, the respondent admitted the lack of a solution led to seeking expert advice to cope with the threat. According to the conceptual framework, if the user perceives that the current threat state is close to the set state of being harmed, the user will then engage in coping mechanisms intended to expand the diminishing state of safety between the threat state and the set state of being hurt (Liang & Xue, 2010).

Response Setback 3: Insufficient technical expertise and skill set among IT security managers. Multiple studies conducted worldwide, such as the Advanced Persistent Threat Awareness, have demonstrated an evident lack of skilled security experts entering the market and a lack of investment in training (Barton, 2019; Carlton, Levy, & Ramim, 2019; He et al., 2019). There is a significant and growing IT security skills shortage (Barton, 2019; Carlton et al., 2019; He et al., 2019). Similarly, respondents in this study felt that security managers lack the skills to identify a data breach and respond promptly. They lack knowledge in compliance, hardware, security software, and security appliances. B-P4 mainly felt that “security managers lacked data communication and persuasion skills to sensitize all the stakeholders on their role in data protection and gain their support.” Respondent A-P6 said, “Security managers lacked SQL database training.”

According to Esplin et al. (2018) and Herold (2017), supported the literature by adding that education leaders and policymakers should place a strong emphasis on security education and awareness training programs and allocate necessary resources that will provide quality technology leadership and professional development for current and future IT professionals. The participants' responses indicated that IT security managers need technical expertise to improve data breach prevention within an organization, including the development of security policies and coordination to ensure specific outcomes. These outcomes include implementing the strategies, anticipating and identifying the potential risk, accessing the business needs and integration of security policies within the business model, providing training related to data security, and knowing how different security protocols should work (Aldawood & Skinner, 2019). A-P1 mentioned the training program called Telnet Training, saying, "They need to at least have a switching protocol that used to be called Telnet Training to understand the simple stuff from IP addresses down to core switch management."

According to three participants (A-P1, A-P6, and B-P2), other necessary skill set requirements that are often lacking among IT security managers are professional certifications, such as a Certified Information Systems Security Professional, that teach basic concepts like baseline configuration, switching protocols, and data security threats. They also needed to be able to develop and implement policies that aligned with the business model and to identify security threats. Two other participants (C-P3 and A-P5) felt it was essential to obtain intelligence reports on data protection threats and mitigation strategies. The first, most essential resource was the institution's data protection policy and documented best practices, as these were in line with the institution's objectives.

According to C-P3, the “skill set that they may or may not have relates to what is the baseline for your network.”

Participants reported attending monthly seminars and conferences to obtain relevant IT skills. Such training is often organized at the school district level and may include webinars such as those held by the Texas Education Agency. As B-P2 stated,

> We have a lot of state resources among educational institutions in Texas. We also do a lot of sharing. TEA [the Texas Education Agency] provides a lot of great information. They normally have a monthly webinar that has pertinent information. I found my peer group to be very beneficial, especially on a regional level.

Another resource was industry-based social groups. Regionally, data security threats follow similar patterns, so networking with local peers, vendors, and data security forums provided security managers with information on the threats they should expect and ideas on how to mitigate them. B-P4 stated,

> I found my peer group to be very beneficial, especially regional. I have worked with friends at local universities and other local institutions in the area to have an informal alert group to say, “Hey, here is what we see here. I am going to be on the watch for this.” And without fail everybody kind of experiences the same thing, in the same period, and then it appears to move on.

The conceptual framework supports this technique that data security and mitigation of data breaches is a technical task that requires specialized technical expertise and skillsets from network security professionals so they can decrease the number of data breaches correctly and promptly (Barton, 2019; Carlton et al., 2019; He et al., 2019).

Theme 4: Recommendations for Strengthening Data Security Prevention and Mitigation Efforts

Recommendations for strengthening data breach prevention and mitigation efforts were the fourth major theme to emerge. Table 6 reveals the frequency of the fourth major theme.

Table 6

Frequency of Fourth Major Theme

	Participants		Document	
Major theme	Count	References	Count	References
Recommendations for strengthening data breach mitigation efforts	6	28	5	12

In the literature, workable strategies found for external attack comprised information security policy, people management, network security, active password policy, antivirus protection and software update, physical security, audit, network security monitoring, data backup, intrusion detection, security education training and awareness (Li et al., 2016). The value of IT security training, education, and security awareness programs were emphasized by Boss et al. (2015), Olusolade Aribake and Mat Aji (2020), and Zwilling et al. (2020). The users of these technologies are just as important as IT security professionals in a technical environment (Taylor-Jackson et al., 2020). Training users and senior managers through structured programming would help mitigate data breaches, as they are sometimes the leading players in these security breaches (Carlton et al., 2019; Da Veiga & Martins, 2015; Dhakal, 2018; Ghazvini & Shukur, 2016; He et al., 2019; Ogbonna, 2020).

Additionally, formulating IT security policies, updating them frequently, and providing guidance to IT professionals on how to respond to data breaches is also crucial to preventing and lessening the frequency of data breaches (Aldawood & Skinner, 2019; Chouhan & Singh, 2016; Furnell, Alotaibi, & Esmael, 2019; Keys & Shapiro, 2019; Kuypers et al., 2016; Pratt-Sensie, 2020). Another strategy is implementing patch management. IT professionals use patches to help update, fix, or improve vulnerabilities that might exist within an organization's network security (Almukaynizi et al., 2019; Jacobs, Romanosky, Adjerid, & Baker, 2019). According to participants, information security without user awareness is the same as closing doors and leaving windows open. Users' ignorance and negligence of information security practices, lack of awareness programs, and lack of or insufficient training are some of the causes of data breaches (Palinkas et al., 2015; Ramalingam et al., 2016). Finally, developing a culture of ongoing capacity development and skill building for IT managers will help in the consistent expansion of IT security managers' knowledge, which could result in more response-ready IT security professionals (Ani, He, & Tiwari, 2019; De Zan, 2019). All participants indicated that IT security managers need to (a) implement ongoing training programs for senior management and users, (b) formulate and update policies, (c) implement patch management, and (d) develop a culture of ongoing capacity development and skill building for IT managers.

Implement ongoing training programs for senior management and users. The participants shared that users' level of awareness on security requirements, roles and responsibilities, and level of compliance determined their activities. Well-designed end-user security training and education can be instrumental in improving organizational internet safety (Ghazvini & Shukur, 2016). One of the respondents, B-P2, recounted that "automation systems design and architecture will always fail if the end user or the human element is not addressed, and education provided because that is your biggest risk." This statement aligned with the decisions by Ghazvini and Shukur (2016) in the literature. All the respondents noted that educating users and management, in general, is one of the essential approaches to implementing proactive data security measures. Trained users are likely to change their online behaviors, comply with the set security policies, and reduce the risk of data breaches. The importance of training emphasized by the participants align with the assertions of Safa et al. (2015).

Respondents also shared that when implementing strategies that prevent a data breach, educating users is the first line of defense. C-P3 said, "Educating the end-user is one of the biggest keys." The views of participants in Case C were supported by Khan, Azam, et al. (2019), who indicated that awareness and training programs are a prevention measure vital in reducing accidental data breaches. The respondents viewed users as the most critical element in the fight against data breaches, as their activities could compromise a high-quality automated system. Most respondents felt that educating users is one of the approaches essential to implementing proactive data security measures. These views of the participants were similar to those presented by Zwilling et al. (2020).

As indicated by Wachyudy (2018) and Safa et al. (2015), trained users are likely to change their online behaviors, comply with the set security policies, and reduce the risk of data breaches.

Similarly, participants felt that information security without user awareness is similar to closing doors but leaving the windows open. User ignorance and negligence of information security practices, lack of awareness programs, and lack of or insufficient training are some of the causes of data breaches (Palinkas et al., 2015; Ramalingam et al., 2016). Many computer users lack sufficient knowledge about information security (Carlton et al., 2019; He et al., 2019). As a result, leaders in both academic institutions and governments need to make extra efforts to provide security awareness to enhance public understanding of cybersecurity risks and threats (Aldawood & Skinner, 2019). IT leaders in a significant number of organizations never carry out continuous security training to help employees spot cyber-attacks, many others do so only when new employees join the company or when there is an incident or an IT threat (Czuprynski & Smith, 2017; Ramalingam et al., 2016; Soomro et al., 2016). Dhakal (2018) indicated that users' level of awareness on security requirements, roles and responsibilities, and level of compliance determined their activities. If the business of an organization involves the storage of data or the conduction of operations online, students or employees in that organization should regularly attend and complete security training initiatives. Continuous employee and student education have a significant impact on protecting data and securing information systems (Aldawood & Skinner, 2019; Raja, 2019).

In addition to educating end-users about how to reduce the chances of causing a breach, IT experts in educational institutions can also rely on technology to keep hackers out but keep access to data open (Bogardus Cortez, 2017). C-P5 stated,

> With human errors, we have to educate our users because . . . we have all these great firewall software, antivirus . . . but at the end of the day, we have to educate our users. They are the ones, ultimately, that will cause the data breach.

In agreement with the conceptual framework when implementing security strategies that prevent a data breach, the human aspect is not to be left out, as it is recognized as one of the root causes of information insecurity. Human error is a critical factor in information security assurance, and a formal security and awareness training program can help minimize its impact (Da Veiga & Martins, 2015; Dhakal, 2018; Ghazvini & Shukur, 2016). Czuprynski and Smith (2017), Furnell and Vasileiou (2017), and Safa et al. (2015), also posited that a well-defined information security training would enhance users' knowledge and lead to a better user behavior and attitude that is geared towards improved_online safety and network security. Additionally, Safa et al. suggested that training targeted at senior management was likely to strengthen ownership and make the managers more involved.

A-P6 recommended "forcing upper management to [take] some security training to help them realize what they are trying to do to help prevent breaches so they can cough out a few extra funds to help us out." The views of A-P6 aligned with recommendations by Esplin et al. (2018) and Herold (2017), who noted that education leaders should place a strong emphasis on security education and awareness training program and allocate necessary resources that will provide quality technology leadership and professional development for current and future IT professionals. Education leaders and policymakers should place a strong emphasis on security education and awareness training programs and allocate the necessary resources that will provide quality technology leadership and professional development for current and future IT professionals (Esplin et al., 2018). These types of education need to span entire school districts from the top down; thus, such training often involves a considerable investment in money, time, and resources, though the advantages and the improvements in the level of security it provides are priceless (Bernstrøm, et al., 2019; Raja, 2019). These training sessions should include information about new and emerging security trends such as rootkits, ransomware, phishing, spyware, denial-of-service attacks, and viruses (Aldawood & Skinner, 2019; Raja, 2019). They could also include training on how to identify fake URLs and phishing e-mail attachments with bogus macro-codes embedded within e-mails to harvest data from a compromised system (Aldawood & Skinner, 2019; Raja, 2019).

Formulate and update policies. It will become more critical for leaders to establish and formulate data security and governance policies that outline how users can safely interact with data by putting policies and procedures in place to stop hackers (Alhassan, Sammon, & Daly, 2019; Bogardus Cortez, 2017). Leaders of industries must implement security policies as best practices in response to new and emerging security threats and comply with U.S. government laws and regulations (Kongnso, 2015). Participants from all three school districts suggested that institutions should always have documented data policies and detail the procedures to follow while responding to data breaches (A-P1, A-P6, B-P2, B-P4, C-P3). IT leaders in organizations should enact policies, design a security framework that consistently classifies information, and act to counter threats and ensure online safety (Boehmer et al., 2015). Soomro et al. (2016) noted the need to review existing security policies and other related details as strategies to leverage to conduct a practical risk assessment for mitigating data breaches.

C-P3 stated,

> Your policies should never be a static document. It should always be changing with the way your users consume data when you bring new products in and when your network changes and how you store data changes. It should be changing all the time.

Thus, in support of the literature, data security policies should be flexible enough to accommodate changes in network and data consumption (Kongnso, 2015). Recent literature supports the findings of this subtheme that security policies should be modified at regular intervals, and employees provided routine and formal training on security (Ramachandran & Chang, 2016). Attackers can maliciously modify security policies if IT experts do not modify them frequently (Oh, Kim, Jeong, Ko, & Kim, 2017).

Implementing policies and best practices will help mitigate data breaches in institutions (Hettiarachchi & Wickramasinghe, 2016). The participants also referred me to the NIST cybersecurity framework policies and procedures because of restrictive information policies. School leaders have mostly faced the challenge of promoting technology, managing, and enacting policies within their school districts (Becker et al., 2017; Herold, 2017). Security control that administratively consists of approved policies, procedures, standards, and guidelines for planning and assessment help reduce and manage risk daily in organizations (Kalaiprasath et al., 2017; Wanyonyi et al., 2017). According to Mishra (2015), security governance defines the direction of information security privacy, policies, and practices within an organization.

Finally, the theme supports the conceptual framework by ensuring that IT security managers formulate and update security policies as safeguarding measures that will be flexible enough to accommodate changes in network and data consumption to help front end user circumvent a threat when they perceive the existence. In all, leaders who fund the IT security process can ensure the productive and practical use of technology resources in enabling an institution to achieve its operational goals (Mishra, 2015).

Patch management. Another recommendation that support the literature is to implement patch management. Patches help update, fix, or improve vulnerabilities within an organization’s network security (Almukaynizi et al., 2019; Jacobs et al., 2019). C-P5 stated that security managers should always work collaboratively with vendors in updating and maintaining both software and hardware. C-P5 advised, “Make sure all your service contracts are up-to-date with your software vendors and your hardware vendors because whenever there is a catastrophic event like that, they are a good resource.” The viewpoints of A-P1, C-P3, and C-P5 aligned with Avery and Wallrabenstein (2018), who indicated that implementing patch management helps IT experts in organizations fix software bugs found on the network. Adamski, Kurowski, Mika, Piątek, and Węglarz (2017) noted that security patches denote an incident that can be handled as a defense against vulnerability to minimize data breaches.

The approach supports the conceptual framework by ensuring that if users perceive their current state is unsafe, they will engage in coping mechanism to enlarge the discrepancy between the current safe state and the undesired end state. Installing software patches as updates can help IT managers respond actively to IT threats and provide normative guidelines to the practical use of deployed IT systems (Boutin, 2015; Josey, 2016; Pereira et al., 2017; Shameli-Sendi et al., 2016). According to Tiainen (2020) and Hayhurst (2018), security breaches are preventable by keeping systems up to date with appropriate patches. Microsoft and other vendors release monthly updates, which IT experts responsible for updates should apply as soon as possible. These updates contain patches that resolve the latest known exploits and vulnerabilities (Li, Rogers, Mathur, Malkin, & Chetty, 2019; Raja, 2019).

Develop a culture of ongoing capacity development and skill building for IT managers. To support the literature, given the fast-changing geography of the internet, there is a growing demand to strengthen cyber capacity beyond national frameworks, and policymakers need to support IT managers of institutions in developing their cybersecurity capacity by enhancing education and technical skills (Calderaro & Craig, 2020). One participant (B-P2) recommended “reaching out to professional organizations . . . because they raise all of our awareness and allow peer groups to share what has worked well for them in their environment.” Nasir, Arshah, Ab Hamid, and Fahmy (2019) found a significant positive relationship between security culture and security knowledge sharing. In developing an ongoing capacity development and skill set development, vendors, contractors, service providers, and partners should work together and be held answerable for keeping online users safe (Stahl & Karger, 2016; Wiley, McCormac, & Calic, 2020). Participants noted that because security managers will not always have answers to all security challenges, it is vital for them to network with industry experts and keep themselves abreast of trends in security threats and data protection strategies.

In supporting the conceptual framework, users can also apply both problems- and emotion-focused coping to reduce IT threats when they recognize the existence of an online threat. Wen, Kianpour, and Kowalski (2019) found a significant positive relationship between security culture and security knowledge sharing. Wen et al. added that a deliberate act that makes knowledge reusable by other people through expertise is about how people share and use what they know and subsequently requires the active engagement of individuals in the process of interaction and learning. Wen et al. emphasized cybersecurity policy and strategy; cyberculture and society; cybersecurity education, training, and skills; and legal and regulatory frameworks, standards, organizations, and technologies as skills for developing cybersecurity capacity (Bellasio et al., 2018). Dutton, Creese, Shillair, Bada, and Roberts (2017) also noted that building cybersecurity capacity is a worthwhile investment.

Applications to Professional Practice

The basis of this study was the perceived lack of strategies used by IT security managers in mitigating data breaches on the network of most schools. According to Loukaka and Rahman (2017), it is challenging for IT security managers to conduct effective network security defense that can prevent or mitigate attacks on their networks if they do not have a sound understanding of vulnerabilities in a system. The findings in the study resulted in some key themes and various insights that IT leaders in other school districts could use as a part of their data security strategies to enhance their system.

The success of any deployed strategy depends on the tools, training, district-leadership buy-in, and security skillset of IT security managers engaged with the responsibility of keeping school technology and students safe online. A sound approach to data security generally exists when procedures and strategies include technical, nontechnical, operational, administrative, and physical controls (Dhakal, 2018; Gatzert & Schmit, 2016; Ghazvini & Shukur, 2016; Li et al., 2016). For a security system to defeat an attack, the system must detect, engage, and neutralize an adversary by response forces (Amundrud et al., 2017). A-P1 and A-P6 mentioned that they rely on training, firewalls, phishing detection software, multifactor authentication, and other technical strategies tailored into their systems as approaches to succeed in the mitigation, protection, and monitoring of information assets. Another essential security technique for the success and growth of the network security framework is awareness among human users (Yousuf, Mahmoud, Aloul, & Zualkernan, 2015).

Two participants noted that they use multiple firewalls so that, in case one fails, the other can do the job. As indicated by Patel (2020), this concept is akin to the understanding that multiple layers of security make it more difficult for an intruder to reach the internal network as the attacker must bypass all the layers to gain access to sensitive data. C-P3 and C-P5 also mentioned the importance of using training and awareness strategies as a way of keeping online users safe, as well as using antivirus software to secure all end-user devices. To reduce the impact or the likelihood of a data breach, IT security managers need to be correctly trained on their responsibilities and be able to train online users, including students, employees, and stakeholders, on how to identify threats and always ensure safety.

Furthermore, the two participants (B-P2 and B-P4), explained that part of their overall mitigation strategies included awareness training and education for students and staff. These explanations aligned with the findings of Rezaeibagha et al. (2015), who reinforced the importance of technical and nontechnical techniques for enhanced IT security and data breach mitigation. Yousuf et al. (2015) added that, for the success and growth of any network security framework, safe online awareness education and training for its users are essential. IT managers of institutions can use these findings to intensify their organization's security policies and strategies in mitigating and securing their data, as they store a lot of identity data, which, when breached, expose valuable assets to cybercriminals.

The findings, therefore, may increase IT security practitioners' understanding and knowledge of the multifaceted structure of cyber-attacks and cybersecurity and may lead to more secure school networks. An effective data security mitigation strategy, when correctly implemented, can benefit IT practice by reducing the number of potential cyber threats, data breaches, and other security incidents on an organization network. When successfully implemented, IT security managers can use such a strategy to break down the complex elements surrounding known and unknown security threats and formulate more effective and appropriate IT guidelines, practices, and policies that will help reduce the negative impact on network performance and online safety. Finally, the strategy will support and provide a more robust framework such that IT leaders responsible for network security will be able to maintain the integrity, authenticity, confidentiality, and nonrepudiation of information on their district network.

Implications for Social Change

Data are at the heart of virtually all institutions, and keeping data protected while facilitating secure usage to drive business value is a crucial success factor. Information technology security managers who use data security strategies enable their organizations to protect their resources, promote digital transformation, comply with regulatory mandates, and generate user trust and loyalty. The growing need to secure sensitive and critical school district data has influenced the development of a variety of solutions, and those to be procured are based on their success in preventing data breaches across various industries**.** The data from the study affirmed the conclusions drawn in the emerged themes are beneficial in the implementation of data security mitigation. School districts have a lot of data on students, parents, and teachers that are valuable to cybercriminals, and the online users and parents whose information may become compromised in a data breach will experience the most negative effects from the breach. The study's findings may influence positive social change that may lead to the online safety of students while accessing their school district network.

The study's findings also show that the participants interviewed agreed on a variety of strategies that will help improve online safety, which included paying attention to students' personal devices accessing the network, enabling multifactor authentication, keeping all district systems updated, and backing up critical data offline. Other suggestions included implementing an institutional security policy by enforcing industry best practices through online user training and phishing campaign awareness, ensuring leadership buy-in and intelligent investment in security, and taking threats seriously. Another suggestion that emerged was that IT security managers should fully understand organizational risk profiles, should ensure the focus of security frameworks is organization needs and should ensure security resources are available to tackle data breaches when they occur. The value this study brings to the community is that community members understand that data fuel organizations, by showing how IT experts can implement strategies to secure their data to ensure confidentiality, integrity, and availability; can conclusively limit the damages that data breaches can cause. Information technology security managers might be able to optimize these mitigation strategies by applying effective data security management strategies that will benefit students, employees, the government, school districts, contracting organizations, and organizational partners. A more secure system serves to build trust and commitment between organizations and their customers, as well as vendors and business partners. Such a relationship could result in increased profitability for an institution. Further, this study may provide societal value by raising IT leaders' awareness about the need to invest wisely in securing school district data because school districts hold a wealth of information that could be valuable to cybercriminals. Finally, organizations with adequate data security assurance strategies build trust, reliability, and confidence that could lead to additional obligations being awarded and to a profitable outcome, resulting in a successful scenario for institutions, IT security managers, students, and parents.

Recommendations for Action

Due to the many choices available for administering online security activities, school district leadership and IT security managers should exercise caution when determining the proper network management tools and the internet safety needs of their users. School district leaders should stipulate security policies and consistently categorize data and controls to ensure users appropriately handle their data categories. Information technology security managers must take ownership of critical data, define the business terms, and track all security control over data quality throughout the data creation process.

Concerning policies, IT security managers should work with school district leadership to coordinate the implementation of standard written IT security procedures and policies and ensure that these policies circulate among peers and online users. School districts should also have a written IT security recovery policy to recover quickly from an incident. Organizational IT leaders should make sure such security policies align with industry best practices. Such policies and procedures should, for instance, include how to handle and authenticate information requests on the creation and enforcement of password changes.

Concerning training, effectively communicating the methods to online users and stakeholders is critical. Leadership must ensure members of the IT security team receive appropriate training on their responsibilities, stay up to date on new and emerging security threats, and obtain outside help when needed from vendors. Information technology security managers need to understand how to identify critical data and prioritize them for proper governances. Information technology security leaders, school personnel, students, and other online users should receive training on how to identify an online threat, mainly through phishing e-mails. They should also ensure that online users learn the best ways to secure their devices, behave responsibly online, and understand what it means to be a good digital citizen. Information technology security managers should ensure stakeholders have the proper training and education on ways to invest wisely in the security of district IT network systems.

Concerning being on the job, school district leaders should provide IT security managers with the tools needed to mitigate data breaches, such as packet monitoring software, to sniff out threats on their network. District leaders should educate students about the robust monitoring tools they have in place that fight against attempted system hacking. IT experts should ensure multifactor authentication are in place and enforced. The physical security of critical network equipment should be visible, implemented, and used. Responsible personnel for software implementation and updates in organizations should also ensure the use of antivirus software on all end-user devices and ensure they are regularly updated. Information technology security managers should restrict access to sensitive data to only those who need access. IT security managers should provide an additional layer of monitoring over traditional filtering and blocking modules that provide safe internet programs. Information technology security managers should have the necessary training and knowledge needed to carry out their job. They should also understand Telnet switching protocol and SQL databases and be familiar with firewall configurations, penetration testing, the security of hardware and software, incident identification and response, and the command-line interface of their network equipment.

Concerning parent assurance, school district leaders should ensure parents are aware of web filter software and tools available within the school district and use it to give parents the ability to monitor their wards' online activities and provide them peace of mind. School district leaders should also implement a strict cross-platform remote monitoring tool, incorporate a form of student training and education about responsible online behavior, administer all devices on the school network in real-time, advance online user knowledge skill on security protocols, use combined infrastructures to provide context by integrating inflexible security measures as insight to help school districts identify potential risks and responses before an incident escalates, minimize the number of remote users to ensure high levels of data security, and embrace a state-of-the-art internet safety technology designed to keep students safe online.

School leadership should enact policies, design a robust security framework that consistently classifies information, and act on counterthreats that will ensure students' online safety (Boehmer et al., 2015). Organization leadership should create internet safety awareness programs among students and parents, as well as discuss online privacy and ethical conduct. Awareness programs for IT security managers administering online activities should involve a student internet safety program that supports compliance with the Children's internet Protection Act. To protect students from cyber threats, IT leaders should educate users on the need to avoid risks, use more than the recommended password length and format, never leave the Wi-Fi access point configuration unchanged, adopt cybersecurity laws and certificate-based access, integrate with access control list (ACLs), layered with encryption.

Moreso, school district leaders should engage third-party firms to provide robust and scalable cloud-based network security management modules for managing devices across school districts. Information technology security managers can safeguard and administer online networks in real-time by monitoring and capturing incident logs of all student activities and flag ups that could be potentially harmful to the network. Also, IT leaders should provide cloud-based network management administration tools designed to help streamline remote networks and improve efficiency and that are authorized to track, remotely monitor, and control devices and users across the entire network on multiple sites across the school district and to simplify network management tasks such as pushing out software updates and endpoint security via a centralized web console. These changes toward action could give organizational leaders a higher sensitivity toward online security and provide institutions with the best practice framework for implementing active online monitoring in schools and expert advice from internet safety partners.

Regarding dissemination, I may distribute the findings of the study through academic journals, industry publications, conferences, training, and workshop. I will provide a strategic summary for data breach mitigation to participants through e-mails so that they can share it various school district leaders and peers. The IT security managers, as the data-breach mitigating expert team, can share the findings with peers within their purview and sphere of influence, as well as others in a broader scope, to enhance the chances of ensuring the implementation of data-breach mitigation strategies within their institutions.

Both my immediate and my long-term goal will be to publish the results of this study and make them available for public searches on data-breach mitigation strategies. I also intend to share the results using appropriate and effective platforms, including my place of work, research websites, IT conferences, college training seminars, the Walden University National Society of Leadership & Success Chapter in the broader research community, and my IT-related LinkedIn groups. Additionally, I plan to build and develop a website, http://drmercynwankwo.com, to present the research findings and possibly create a resource center for updates to new and emerging security threats and how IT security managers can leverage on emerging strategies.

Recommendations for Further Study

The internet has become an ideal place for criminals and terrorists to carry out their misdeeds. Recent assessments of the data security breach landscape show that no industry segment is immune to cyber-attacks, and educational institutions top the list for targeted security incidents due to the sensitive information that they house. These fears are justified, especially as large and small organizations continue to suffer threats regularly and because of the constant cycle of data breach news, even in large corporations, despite their heavy controls. The implication of this perpetual cycle of data breaches is that technical solutions alone do not constitute a complete solution to data breach problems and that data breaches can be devastating. Leaders of school districts and IT security managers are conscious of the gravity of the problem and the associated implications, but so are cybercriminals. A significant contribution from this study is the creation of security awareness and strategic approach to threat mitigation, threat acceptance, threat avoidance, and understanding the needs and resources that require consideration in securing schools' networks. IT leaders in institutions must identify and prioritize critical data for proper governance. A systematic implementation approach is essential. Therefore, researchers should investigate the element of data security threats that impair school networks further to determine IT security managers' perceptions concerning this subject and the best system approach moving forward as new hacking techniques evolve.

The limitations of this study were primarily the study sample size and data availability. The outcomes depended on participant experiences. To increase the chance that IT research meets the level of experiences of research participants, I recommend that researchers interview other IT security professionals such as network engineers, IT security analysts, and school district leaders to gain their views and possibly evaluate different findings. Another recommendation is to expand the population to include the stakeholders, general district leaders in the institutions, and subject matter experts or data owners in future research.

Another limitation is that IT security managers use different or multiple technologies, strategies, and procedures for monitoring online activities, which render making any generalizations to school network security challenges. I recommend that institution leadership invest intelligently in safety and take IT threats seriously by providing an organizational best practice framework for implementing active online monitoring in schools and seek expert advice from internet safety partners. Information technology security managers and leaders of school districts understand the structure of the IT security infrastructure of their network and potentially scarce resources before proposing monitoring tools to the leadership team.

Another limitation is that the study result may not be generalized to the entire United States since the study participants were limited to the state of Texas. This study was limited to cybersecurity and data breach issues facing three school districts in the state of Texas, as data collected for cybersecurity threats in one school district may differ from the data gathered from participants in another school district. I recommend conducting future research by expanding the geographical area first to a region versus a state to broaden the understanding of data breaches in a region. Scaling the study down to include IT security managers or up to cover large school districts extends the context of knowledge to the data breach mitigation strategies used in school districts in different states.

Another limitation was that networks, data breaches, and cybersecurity are not only broad and expanding topics but also serve as a source of fear to many leaders of educational institutions. I recommend that educational institutions show greater transparency through data-breach notification laws, be held accountable, and be given more significant incentives to invest. I also recommend periodic IT risk assessment on district networks. An IT risk assessment is a comprehensive review of an IT infrastructure of an organization, intending to identify existing flaws to exploit to threaten the security of the network and data. The risk assessment serves as a basis for deciding what countermeasures, if any, to take to reduce risk to an acceptable level, based on the value of the information resource to the organization. I also recommend that IT security managers within school districts explore other cybersecurity data breach safe practices and control attempts for mitigation data breaches in different sectors such as banking, health, and other government agencies.

Reflections

No research is free from assumptions, biases, and the personality of the researcher (Roulston & Shelton, 2015). According to Semenova and Hassel (2015), assumptions and biases constitute external factors that may influence a researcher's inquiry. According to Twining et al. (2017), assumptions surface when the general expectations of a researcher direct the investigative conclusion of the study. During this research, I had a set of preconceived ideas, viewpoints, biases, and assumptions. I assumed that my participants would provide error-free responses to my interview questions and that collated data would be a suitable representation of the strategies deployed by IT security managers for mitigating cybersecurity threats in schools. Individual viewpoints may potentially shape the path of research, and thus researchers should provide reliable and supportive theoretical frameworks while conveying personal insights (Mortari, 2015).

Ardagna et al. (2015) recommended that researchers consider participants in qualitative research as experts in the areas relevant to the study. I preconceived the idea that the IT security managers who would participate in my research would have adequate experiences in mitigating cybersecurity threats on their networks. However, my thinking changed as this study concludes. For instance, the responses from study participants may have reflected views that were in the best interest of their school or may have undermined their possible job inexperience in a self-reporting partisan way. Furthermore, IT security managers may use different or multiple technologies, strategies, and procedures for monitoring online activities, which renders making any generalizations regarding the best approach to school network security challenging.

Summary and Study Conclusions

Data breaches are a constant threat to organizations, and school districts are a prime target as they store a lot of valuable information. The absence of an actual data breach experience across the three school districts does not mean the absence of a threat, and it does not also make IT security managers feel that their institutions are less susceptible to a data breach incident. Data security is dynamic, evolving, and continues to advance in time. Cyber threats will continue to occur as long as technology continues to be utilized. The increases in data security breaches create a sense of urgency for IT security managers to take measures to safeguard district networks. In this study, I applied the framework of the TATT to evaluate what, why, and how IT security managers try to avoid or limit data security breaches in their networks and the behavior they exhibit when they perceive a threat to their systems culminating in the strategies they use in threat mitigation for their organization.

The successful implementation of these strategies involves not only the technology but also people and processes. The people aspect of the strategy entails the willingness of district leaders to buy into the strategic recommendations of the IT security managers and the capability of the managers to communicate the importance of those security needs adequately. Organization leadership must be engaged and brought in to explore how best to invest intelligently in school district security and take threats seriously by exercising caution when subscribing to network management tools and internet safety needs of school networks. Such a subscription may include the continual cyber training of users on the proper use of technology, ongoing education on the tactics used by hackers, and the establishment of policies and procedures for password use, change management, and ethical rules that guide the general IT infrastructure. IT managers should also ensure that access policy to school district sensitive data is established and followed, allowing access to only those who need it.

Information technology security managers must safeguard data, update IT security procedures, destroy data before disposal, educate and train online users, control computer use, and secure all computers. Although IT security managers may not have a solution to every IT security problem that arises, they must understand vulnerabilities in a system, or it will be challenging to conduct effective network security defense to prevent attacks. It is essential to monitor and capture incidents logs of all student activities connected remotely to the network and flag up in real-time activities that could be potentially harmful to the network. District leaders and IT security managers must understand that data security means knowing about their data and about threats to their data and controlling the consequences associated with those risks through safeguarding, monitoring, ownership, accountability, and investigating the movement of the data. The focus of these strategies is on countering threats to data, mitigating risks, understanding data breaches, providing monitoring and preventive processes, and establishing notification procedures when breaches occur. The need to protect school district networks is not a static event that occurs within a specific space of time. Information technology managers must continue to monitor and safeguard data through the strategic use of people, processes, procedures, partners, and technology.

References

Abraham, C., & Sheeran, P. (2017). Implications of goal theories for the theories of reasoned action and planned behavior. In C. J. Armitage & J. Christian (Eds.), *Planned behavior* (pp. 101-122). Routledge. doi:10.4324/9781315126449-7

Adamovic, S., Sarac, M., Stamenkovic, D., & Radovanovic, D. (2018). The importance of using software tools for learning modern cryptography. *International Journal of Engineering Education*, *34*(1), 256-262.

Adamski, M., Kurowski, K., Mika, M., Piątek, W., & Węglarz, J. (2017). Security aspects in resource management systems in distributed computing environments. *Foundations of Computing and Decision Sciences*, *42*(4), 299-313. doi:10.1515/fcds-2017-0015.

Ahmadvand, M., Pretschner, A., Ball, K., & Eyring, D. (2018). Integrity protection against insiders in microservice-based infrastructures: From threats to a security framework. *Federation of International Conferences on Software Technologies: Applications and Foundations, 43,* 573-588. doi:10.1007/978-030-0477/9-43

Ajzen, I. (2015). The theory of planned behaviour is alive and well, and not ready to retire: A commentary on Sniehotta, Presseau, and Araújo-Soares. *Health Psychology Review, 9*, 131-137. doi:10.1080/17437199.2014.883474

Alam, T., & Hamid, K. (2018). *Implementation of DYNAMIC MULTIPOINT VPN over IPsec for Secure Enterprise Network* [Doctoral dissertation, IIUC Central Library]. International Islamic University Chittagong Digital Archive.

http://dspace.iiuc.ac.bd:8080/xmlui/bitstream/handle/88203/306/IIUC-ETE-Report-04.pdf?sequence=1&isAllowed=y

Al-Daeef, M. M., Basir, N., & Saudi, M. M. (2017). Security awareness training: A review. *Proceedings of the World Congress on Engineering 1*, 5-7. http://www.iaeng.org

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future internet*, *11*(3). doi:10.3390/fi11030073

Alhassan, I., Sammon, D., & Daly, M. (2019). Critical success factors for data governance: A theory-building approach. *Information Systems Management*, *36*(2), 98-110. doi:10.1080/10580530.2019.1589670

Alhassan, J. K., Misra, S., Umar, A., Maskeliūnas, R., Damaševičius, R., & Adewumi, A. (2018, January). A fuzzy classifier-based penetration testing for web applications. In *International Conference on Information Theoretic Security* (pp. 95-104). Springer.

Ali, B., & Awad, A. (2018). Cyber and physical security vulnerability assessment for IoT-based smart homes. *Sensors*, *18*(3), 817. doi:10.3390/s18030817

Al-khatib, A. A., & Hassan, R. (2018). Impact of IPSec protocol on the performance of network real-time applications: A review. *IJ Network Security*, *20*(5), 811-819. http://ijns.jalaxy.com.tw/contents/ijns-v20-n5/ijns-2018-v20-n5-p811-819.pdf

Almukaynizi, M., Nunes, E., Dharaiya, K., Senguttuvan, M., Shakarian, J., & Shakarian, P. (2019). Patch before exploited: An approach to identify targeted software vulnerabilities. In *AI in cybersecurity* (pp. 81-113). Springer.

Alreemy, Z., Chang, V., Walters, R., & Wills, G. (2016). Critical success factors (CSFs) for information technology governance (ITG). *International Journal of Information Management, 36*, 907-916. doi:10.1016/j.ijinfomgt.2016.05.017

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies*, *82*, 69-82. doi:10.1016/j.ijhcs.2015.05.005

Al-Sohbani, Y. A. Y. (2016). An investigation of the reasons behind the weaknesses in English among public secondary school leavers. *Journal of Teaching and Teacher Education*, *4*, 41-51. doi:10.12785/jtte/040105

Althonayan, A., & Andronache, A. (2018, September 22). Shifting from information security towards a cybersecurity paradigm. In *Proceedings of the 2018 10th International Conference on Information Management and Engineering*, Salford, U.K (pp. 68-79). doi:10.1145/3285957.3285971

Amankwaa, L. (2016). Creating protocols for trustworthiness in qualitative research. *Journal of Cultural Diversity*, *23*(3), 121-127. doi:10.1177/JCD-2015-0015

Amundrud, Ø., Aven, T., & Flage, R. (2017). How the definition of security risk can be made compatible with safety definitions. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, 231*, 286-294. doi:10.1177/1748006X17699145

Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: Evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology*, *21*(1), 2-35. doi:10.1108/JSIT-02-2018-0028

Antwi, S. K., & Hamza, K. (2015). Qualitative and quantitative research paradigms in business research: A philosophical reflection. *European Journal of Business and Management*, *7*, 217-225. doi:10.1088/EJBM-01-2014-0015

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38,* 304-312. doi:10.1016/j.chb.2014.05.046

Arachchilage, N. A. G., Love, S., & Beznosov, K. (2016). Phishing threat avoidance behaviour: An empirical investigation. *Computers in Human Behavior, 60*, 185-197. doi:10.1016/j.chb.2016.02.0650747-5632/

Ardagna, C. A., Asal, R., Damiani, E., & Vu, Q. H. (2015). From security to assurance in the cloud: A survey. *ACM Computing Surveys (CSUR)*, *48*(1), 1-50. doi:10.1145/2767005

Arpaci, I. (2016). Understanding and predicting students’ intention to use mobile cloud storage services. *Computers in Human Behavior*, *58*, 150-157. doi:10.1016/j.chb.2015.12.067

Atapour-Abarghouei, A., Bonner, S., & McGough, A. S. (2019, December). A king’s ransom for encryption: Ransomware classification using augmented one-shot learning and Bayesian approximation. In *2019 IEEE International Conference on*

Big Data (Big Data) (pp. 1601-1606). IEEE. doi:10.1109/BigData47090.2019.9005540

Avery, J., & Wallrabenstein, J. R. (2018). Formally modeling deceptive patches using a game-based approach. *Computers & Security*, *75*, 182-190. doi:10.1016/j.cose.2018.02.009

Babar, A., & Ullah, R. (2019). Tax collection system. *Scientific and Technical Reports*, *1*(1), 1-43. Retrieved from https://aswapublishers.org/index.php/str/article/download/1/2

Baillie, L. (2015). Promoting and evaluating scientific rigour in qualitative research. *Nursing Standard*, *29*(46), 36-42. doi:10.7748/ns.29.46.36.e8830

Bakar, Z. A., Yaacob, N. A., Udin, Z. M., Hanaysha, J. R., & Loon, L. K. (2017). The adoption of business continuity management best practices among Malaysian organizations. *Advanced Science Letters*, *23*, 8484-8491. doi:10.1166/asl.2017.9916

Balozian, P., & Leidner, D. (2017). Review of IS security policy compliance. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems, 48*(3), 11-43. doi:10.1145/3130515.3130518

Bamkin, M., Maynard, S., & Goulding, A. (2016). Grounded theory and ethnography combined*. Journal of Documentation*, *72*, 214-231. doi:10.1108/jd-01-2015-0007

Barden, M. (2020). *FBI investigating after Manor ISD loses $2.3M in phishing email scam.* Retrieved from https://web.archive.org/web/20200111153128/https://news4sanantonio.com/news/local/fbi-investigating-after-manor-isd-loses-23m-in-phishing-email-scam

Barnes, J. (2017). Qualitative research from start to finish (2nd ed.). *Neuropsychological Rehabilitation*, *27*, 1156-1158. doi:10.1080/09602011.2015.1126911

Barnham, C. (2015). Quantitative and qualitative research: Perceptual foundations. *International Journal of Market Research*, *57*, 837-854. doi:10.2501/IJMR-2015-070

Barton, D. (2019). *The cybersecurity talent gap = an industry crisis.* Retrieved from https://www.securitymagazine.com/articles/90182-the-cybersecurity-talent-gap-an-industry-crisis

Barton, K. A., Tejay, G., Lane, M., & Terrell, S. (2016). Information system security commitment: A study of external influences on senior management. *Computers & Security*, *59*, 9-25. doi:10.1016/j.cose.2016.02.007

Becker, S. A., Cummins, M., Davis, A., Freeman, A., Hall, C. G., & Ananthanarayanan, V. (2017). *NMC horizon report: 2017 higher education edition* (pp. 1-60). New Media Consortium.

Belanger, K., Buka, S., Cherry, D. C., Dudley, D. J., Elliott, M. R., Hale, D. E., & Triche, E. W. (2013). Implementing provider-based sampling for the national children's study: Opportunities and challenges. *Paediatric and Perinatal Epidemiology*, *27*, 20-26. doi:10.1111/ppe.12005

Bellasio, J., Flint, R., Ryan, N., Sondergaard, S., Monsalve, C. G., Meranto, A. S., & Knack, A. (2018). Developing cybersecurity capacity: A proof-of-concept implementation guide. doi:10.7249/RR2072

Bello Garba, A., 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. http://www.arpnjournals.com/jeas/research_papers/rp_2015/jeas_0215_1591.pdf

Benjelloun, F. Z., & Lahcen, A. A. (2019). Big data security: Challenges, recommendations, and solutions. *Web Services: Concepts, Methodologies, Tools, and Applications*, *2*, 25-38. doi:10.1177/DMTA-05-2018-0001

Berger, R. (2015). Now I see it, now I don’t: Researcher’s position and reflexivity in qualitative research. *Qualitative Research*, *15*, 219-234. doi:10.1177/1468794112468475

Bernstrøm, V. H., Drange, I., & Mamelund, S. E. (2019). Employability as an alternative to job security. *48*(1), 234-248. doi:10.1108/PR-09-2017-0279

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance-Issues and Practice*, *40*, 131-158. doi:10.1057/gpp.2014.19

Birt, L., Scott, S., Cavers, D., Campbell, C., & Walter, F. (2016). Member checking: A tool to enhance trustworthiness or merely a nod to validation? *Qualitative Health Research*, *26*, 1802-1811. doi:10.1177/1049732316654870

Blake, L., Francis, V., Johnson, J., Khan, M., & McCray, T. (2017). Developing robust data management strategies for unprecedented challenges to healthcare information. *Journal of Leadership, Accountability, and Ethics*, *14*, 22-31. doi:10.1057/JLAE-01-2016-0125

Bliese, P. D., Edwards, J. R., & Sonnentag, S. (2017). Stress and well-being at work: A century of empirical trends reflecting theoretical and societal influences. *Journal of Applied Psychology, 102*, 389-402. doi:10.1037/apl0000109

Boddy, C. R. (2016). Sample size for qualitative research. *Qualitative Market Research: An International Journal*, *19*, 426-432. doi:10.1108/QMR-06-2016-0053

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*, 1022-1035. doi:10.1080/0144929X.2015.1028448

Bogardus Cortez, M. (2017). *Education sector data breaches skyrocket in 2017.* Retrieved from https://edtechmagazine.com/higher/article/2017/12/education-sector-data-breaches-skyrocket-2017

Bolkan, J. (2017). *Education data breaches double in first half of 2017.* Retrieved from https://campustechnology.com/articles/2017/09/20/education-data-breaches-double-in-first-half-of-2017.aspx

Boss, S., Galletta, D., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly, 39*, 837-864. doi:10.1108/MQ-02-2014-0001

Boutin, D. (2015). *The Big 3: Why change, release, and configuration management are key to performance engineering.* Retrieved from https://www.axelos.com/news/blogs/november-2015/the-big-3-change-release-configuration-management

Boynton, A. C., Zmud, R. W., & Jacobs, G. C. (1994). The influence of IT management on IT use in large organizations. *MIS Quarterly*, 299-318. doi:10.1108/MQ-02-1993-0002

Braga, A., & Dahab, R. (2015). A survey on tools and techniques for the programming and verification of secure cryptographic software. In Anais do XV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais. *Proceedings of XV SBSeg*, 30-43. Florianópolis, SC, Brazil.

Braganza, M., Akesson, B., & Rothwell, D. (2017). An empirical appraisal of Canadian doctoral dissertations using grounded theory: Implications for social work research and teaching. *Journal of Teaching in Social Work*, *37*, 528-548. doi:10.1080/08841233.2017.1386259

Braun, V., Clarke, V., Hayfield, N., & Terry, G. (2019). Thematic analysis. In *Handbook of research methods in health social sciences* (pp. 843-860). Springer. doi:10.1007/978-981-10-5251-4_103

Buchler, N., La Fleur, C. G., Hoffman, B., Rajivan, P., Marusich, L., & Lightner, L. (2018). Cyber teaming and role specialization in a cyber security defense competition. *Frontiers in Psychology, 9*, 2133. doi:10.3389/fpsyg.2018.02133

Buckman, J., Bockstedt, J., Hashim, M. J., & Woutersen, T. (2017). *Do organizations learn from a data breach?* Paper presented at the 16th Annual Workshop on the Economics of Information Security (WEIS), San Diego, CA.

Butts, S. (2016). *Midway students charged with false report, using forged document.* Retrieved from https://www.wacotrib.com/news/education/midway-students-charged-with-false-report-using-forged-document/article_cc2374e1-778b-5409-887a-db6a7cfbb4cc.html

Calderaro, A., & Craig, A. J. (2020). Transnational governance of cybersecurity: Policy challenges and global inequalities in cyber capacity building. *Third World Quarterly*, 41(6), 1-22. doi:10.1080/01436597.2020.1729729

Canales, J. I. (2015). Sources of selection in strategy making. *Journal of Management Studies*, *52*, 1-31. doi:10.1111/joms.12101

Carlton, M., Levy, Y., & Ramim, M. (2019). Mitigating cyber attacks through the measurement of non-IT professionals' cybersecurity skills. *Information & Computer Security*. *27*(1), 101-121. doi:10.1108/ICS-11-2016-0088

Carpenter, D., Young, D. K., Barrett, P., & McLeod, A. J. (2019). Refining technology threat avoidance theory. *Communications of the Association for Information Systems*, *44*(1), 22. doi:10.17705/1CAIS.04422

Carver, C. S., & Scheier, M. F. (1982). Control theory: A useful conceptual framework for personality–social, clinical, and health psychology. *Psychological Bulletin, 92*, 111. doi:10.1037/0033-2909.92.1.111

Castleberry, A., & Nolen, A. (2018). Thematic analysis of qualitative research data: Is it as easy as it sounds? *Currents in Pharmacy Teaching and Learning, 10,* 807-815. doi:10.1016/j.cptl.2018.03.019

Chapman, J. (2019). *How safe is your data? Cyber-security in higher education.* Higher Education Policy Institute.

Chase, E. (2017). Enhanced member checks: Reflections and insights from a participant-researcher collaboration. *Qualitative Report*, *22*, 2689-2703.

Chaudhry, S. A. (2016). A secure biometric based multi-server authentication scheme for social multimedia networks. *Multimedia Tools and Applications*, *75*, 12705-12725. doi:10.1007/s11042-015-3194-0

Cheng, L., Liu, F., & Yao, D. D. (2017). Enterprise data breach: Causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 7*(5), 1-14. doi:10.1002/widm.1211

Chiong, W., Leonard, M. K., & Chang, E. F. (2017). Neurosurgical patients as human research subjects: ethical considerations in intracranial electrophysiology research. *Neurosurgery*, *83,* 29-37. doi:10.1093/neuros/nyx361

Chipp, T. (2016). Ransomware attack hits Texas education service district. Six school district websites went down as attackers blocked access to computer systems.

Retrieved from https://www.govtech.com/education/k-12/Ransomware-Attack-Hits-Texas-Education-Service-District.html

Chopra, A. (2016). Security Issues of Firewall. *International Journal of P2P Network Trends and Technology (IJPTT)*, *22*(1), 4-9. doi:10.14445/22492615/IJPTT-V22P402

Chouhan, P., & Singh, R. (2016). Security attacks on cloud computing with possible solution. *International Journal of Advanced Research in Computer Science and Software Engineering*, *6*(1), 92–96. doi:10.1177/IJARCSSE-2015-0012

Cochran, J. D., Baker, H. M., Benson, D., & Rhea, W. (2016). Business student perceptions of online learning: Using focus groups for richer understanding of student perspectives. *Organization Management Journal*, *13*(3), 149-166. doi:1080/15416518.2016.1218195

Collins, M. D., Jackson, C. J., Walker, B. R., O'connor, P. J., & Gardiner, E. (2017). Integrating the context-appropriate balanced attention model and reinforcement sensitivity theory: Towards a domain-general personality process model. *Psychological Bulletin*, *143*, 91-112. doi:10.5172/mra.2013.7.2.271

Colorafi, K. J., & Evans, B. (2016). Qualitative descriptive methods in health science research. *HERD: Health Environments Research & Design Journal*, *9*(4), 16-25.

Connelly, L. M. (2016). Trustworthiness in qualitative research. *Medsurg Nursing*, *25*(6), 435-437. doi:10.1177/MN-2015-0001

Cooperrider, D., & Srivastva, S. (2017). Appreciative inquiry in organizational life. *Research in Organizational Change and Development*, *2,* 81-142. doi:10.1177/ROCD-2016-1100

Coppolino, L., D'Antonio, S., Mazzeo, G., & Romano, L. (2017). Cloud security: Emerging threats and current solutions. *Computers & Electrical Engineering*, *59*, 126-140. doi:10.1016/j.compeleceng.2016.03.004

Crandall, C. S., & Sherman, J. W. (2016). On the scientific superiority of conceptual replications for scientific progress. *Journal of Experimental Social Psychology*, *66*, 93-99. doi:10.1016/j.jesp.2015.10.002

Cronin, C. J., & Lowes, J. (2016). Brief encounters with qualitative methods in health research: Phenomenology and interpretative phenomenological analysis. *Cumbria Partnership Journal of Research Practice and Learning*, *5*, 8-12. http://researchonline.ljmu.ac.uk/id/eprint/1292/

Crowley ISD. (2018). *Statement regarding fraud investigation.* Retrieved from https://www.crowleyisdtx.org/site/default.aspx?PageType=3&DomainID=4&ModuleInstanceID=6022&ViewID=6446EE88-D30C-497E-9316-3F8874B3E108&RenderLoc=0&FlexDataID=8729&PageID=1

Cunha, M. L. (2018). *Privacy rights for families and children in k-12 schools: A mixed methods study on the effects of perceptions of educators on implementation of the family educational rights and privacy act (FERPA)* [Doctoral dissertation, Concordia University Irvine]. Concordia University Library. Retrieved from https://cui.dspacedirect.org/bitstream/handle/11414/3345/Cunha%20Final%20Dissertation.pdf?sequence=1&isAllowed=y

Czuprynski, C. N., & Smith, R. (2017). *Data security for schools: A legal and policy guide for school boards.* National School Boards Association. Retrieved from https://cdn-files.nsba.org/s3fs-public/reports/Data_Security_Guide_5_Jan2017.pdf

Daman, R., & Tripathi, M. M. (2015). Encryption tools for secured health data in public cloud. *International Journal of Innovative Science, Engineering & Technology, 2*(11), 843–848. doi:10.24237/djps.1401.205C

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*, 281-297. doi:10.1016/j.cose.2014.11.002

Darwazeh, N. S., Al-Qassas, R. S., & AlDosari, F. (2015). A secure cloud computing model based on data classification. *Procedia Computer Science, 52*, 1153-1158. doi:10.1016/j.procs.2015.05.150

Das, A., & Khan, H. U. (2016). Security behaviors of smartphone users. *Information & Computer Security, 24*, 116-134. doi:10.1108/ICS-04-2015-0018

Da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security, 49*, 162-176. doi:10.1016/j.cose.2014.12.006

De Guinea, A. O., & Webster, J. (2017). Combining variance and process in information systems research: Hybrid approaches. *Information and Organization, 27*(3), 144-162. doi:10.1108/IO-2016-00145

Demers, G., Harrington, S., Cianci, M., & Green, N. (2017). Protecting colleges & universities against real losses in a virtual world. *John Marshall Journal of Information Technology & Privacy Law*, *33*(2), 3-22. doi:10.1008/JMJITPL-2016-0011

Derouet, E. (2016). Fighting phishing and securing data with email authentication. *Computer Fraud & Security, 2016*(10), 5-8. doi:10.1016/S1361-3723(16)30079-3

Dev, H., & Liu, Z. (2017). Identifying frequent user tasks from application logs. In *Proceedings of the 22nd International Conference on Intelligent User Interfaces* (pp. 263-273). doi:10.1145/3025171.3025184

Dey, D., Ghoshal, A., & Lahiri, A. (2018, January 03). Security circumvention: To educate or to enforce?. In *Proceedings of the 51st Hawaii International Conference on System Sciences*. doi:10.24251/HICSS.2018.648

De Zan, T. (2019). *Mind the gap: The cyber security skills shortage and public policy interventions.* Retrieved from https://gcsec.org/mind-the-gap-the-cyber-security-skills-shortage-and-pubblic-policy-interventions-2/

Dhakal, R. (2018). *Measuring the effectiveness of an information security training and awareness program.* Retrieved from https://researchoutput.csu.edu.au/ws/portalfiles/portal/27678937/Roshan_Dhakal_Completed_DIT_Thesis.pdf

Dillaway, H., Lysack, C., & Luborsky, M. R. (2017). Qualitative approaches to interpreting and reporting data. In R. R. Taylor (Ed.), *Kielhofner's research in occupational therapy: Methods of inquiry for enhancing practice* (2nd ed., pp. 229-243). F.A. Davis Company

DiMase, D., Collier, Z. A., Heffner, K., & Linkov, I. (2015). Systems engineering framework for cyber physical security and resilience. *Environment Systems and Decisions*, *35*, 291-300. doi:10.1007/s10669-015-9540-y

Dimitrova, B., & Mileva, A. (2017). Steganography of Hypertext Transfer Protocol Version 2 (HTTP/2). *Journal of Computer and Communications*, *5*, 98-111. doi:10.4236/jcc.2017.55008

Dion, E. (2017). *Bay School District website hacked, replaced with anime character.* Retrieved from https://www.nwfdailynews.com/news/20170724/bay-school-district-website-hacked-replaced-with-anime-character?template=ampart

Doody, O., & Noonan, M. (2016). Nursing research ethics, guidance and application in practice. *British Journal of Nursing*, *25*(14), 803-807. doi:10.12968/bjon.2016.25.14.803

Durrant, G., Moore, J., Correa, S., & Smith, P. (2016). *Assessing risk of nonresponse bias and dataset representativeness during survey data collection.* http://eprints.ncrm.ac.uk/3786/1/Maintaining%20high%20response%20rates%20%E2%80%93%20is%20it%20worth%20the%20effort%20-%20G%20Durrant.pdf

Durumeric, Z., Adrian, D., Mirian, A., Kasten, J., Bursztein, E., Lidzborski, N., ... & Halderman, J. A. (2015). Neither snow nor rain nor MITM... an empirical analysis of email delivery security. In *Proceedings of the 2015 Internet Measurement Conference* (pp. 27-39). New York, NY, USA, 2015. ACM. doi:10.1145/2815675.2815695

Dutton, W. H., Creese, S., Shillair, R., Bada, M., & Roberts, T. (2017). *Cyber security capacity: Does it matter?* Retrieved from https://www.researchgate.net/profile/Ruth_Shillair/publication/319645577_Cyber_Security_Capacity_Does_it_Matter/links/59b7cdf4458515c212b505a3/Cyber-Security-Capacity-Does-it-Matter.pdf

Elkabbany, G. F., & Rasslan, M. (2018). Security issues in distributed computing system models. *Cyber security and threats: Concepts, methodologies, tools, and applications* (pp. 381-418). IGI Global. doi:10.4018/978-1-5225-5634-3.ch022

Elmrabit, N., Yang, S. H., & Yang, L. (2015). Insider threats in information security categories and approaches. *2015 21st International Conference on Automation and Computing (ICAC)* (pp. 1-6). IEEE. doi:10.1109/IConAC.2015.7313979

Eltayeb, M., & Dawson, M. (2016). Understanding user's acceptance of personal cloud computing: Using the technology acceptance model. In *Information technology: New generations* (pp. 3-12). Springer. doi:10.1007/978-3-319-32467-8_1

Esplin, N. L., Stewart, C., & Thurston, T. N. (2018). Technology leadership perceptions of Utah elementary school principals. *Journal of Research on Technology in Education*, *50*, 305-317. doi:10.1080/15391523.2018.1487351

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics, 5*, 1-4. doi:10.1164/j.ajtas.20160501.11

Federal Bureau of Investigation. (2016). *Law Enforcement Enterprise Portal (LEEP). 2016 internet crime report.* Retrieved from https://pdf.ic3.gov/2016_IC3Report.pdf

Fenner, M. R., Jr. (2017). *The relationship between technology threat avoidance and innovation in health care organizations* [Doctoral dissertation, Walden University]. ScholarWorks. http://scholarworks.waldenu.edu/dissertation

Fernández-Alemán, J. L., García, A. B. S., García-Mateos, G., & Toval, A. (2015). Technical solutions for mitigating security threats caused by health professionals in clinical settings. *Conference Proceedings in Medicine and Biology, 2015,* 1389-1392. doi:10.11648/j.ajtas.20160501.11

Fink, G., Edgar, T., Rice, T., MacDonald, D., & Crawford, C. (2017). Security and privacy in cyber-physical systems. In Intelligent Data-Centric Systems (Editors.), *Cyber-physical systems* (pp. 129-141). doi:10.1016/b978-0-12-803801-7.00009-2

Fink, K., & Anderson, C. W. (2015). Data journalism in the United States. *Journalism Studies, 16*, 467-481. doi:10.1080/1461670x.2014.939852

Force, J. T. (2017). *Security and Privacy Controls for Information Systems and Organizations* (NIST Special Publication (SP) 800-53 Rev. 5 (Draft)). National Institute of Standards and Technology.

Foster, I. D., Larson, J., Masich, M., Snoeren, A. C., Savage, S., & Levchenko, K. (2015, October 15). Security by any other name: On the effectiveness of provider based email security. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver Colorado USA October,* (pp. 450-464). doi:10.1145/2810103.2813607

Frank, R., & Wagner, L. (2018). *Understanding the importance of FERPA & data protection in higher education.* Retrieved from https://digitalcommons.lassalle.edu/mathcompcapstones/36

Franke, M. L., Turrou, A. C., Webb, N. M., Ing, M., Wong, J., Shin, N., & Fernandez, C. (2015). Student engagement with others' mathematical ideas: The role of teacher invitation and support moves. *Elementary School Journal*, *116*, 126-148. doi:10.1086/683174

Frels, R. K., & Onwuegbuzie, A. O. (2013). Administering quantitative instruments with qualitative interviews: A mixed research approach. *Journal of Counseling and Development*, *91*, 2-15. doi:10.1108/JCD-02-2012-0014

Friesen, P., Kearns, L., Redman, B., & Caplan, A. L. (2017). Rethinking the Belmont report? *American Journal of Bioethics, 17*(7), 15-21. doi:10.1080/15265161.2017.1329482

Fuller, D., Shareck, M., & Stanley, K. (2017). Ethical implications of location and accelerometer measurement in health research studies with mobile sensing devices. *Social Science & Medicine, 191*, 84-88. doi:10.1016/j.socscimed.2017.08.043

Furnell, S., Alotaibi, F., & Esmael, R. (2019, January 08). Aligning security practice with policy: Guiding and nudging towards better behavior. In *Proceedings of the 52nd Hawaii International Conference on System Sciences* (HICSS), 5618–5627. Maui, Hawaii. doi:10.24251/HICSS.2019.676

Furnell, S., & Vasileiou, I. (2017). Security education and awareness: Just let them burn? *Network Security*, *12*, 5-9. doi:10.1016/S1353-4858(17)30122-8

Fusch, P., Fusch, G. E., & Ness, L. R. (2018). Denzin’s paradigm shift: Revisiting triangulation in qualitative research. *Journal of Social Change*, *10*, 19-32. doi:10.5590/JOSC.2018.10.1.02

Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *Qualitative Report*, *20*, 1408-1416. http://www.nova.edu/sss/QR/QR20/9/fusch

Gadinger, F., & Peters, D. (2016). Feedback loops in a world of complexity: A cybernetic approach at the interface of foreign policy analysis and international relations theory. *Cambridge Review of International Affairs*, *29*, 251-269. doi:10.1080/09557571.2013.872599

Gamachchi, A., & Boztas, S. (2017). Insider threat detection through attributed graph clustering. In *2017 IEEE Trustcom/BigDataSE/ICESS*, *4*, 112-119. doi:10.1109/Trustcom/BigDataSE/ICESS.2017.227

Gangwar, H., & Date, H. (2016). Critical factors of cloud computing adoption in organizations: An empirical study. *Global Business Review*, *17*, 886-904. doi:10.1177/0972150916645692

Gatzert, N., & Schmit, J. (2016). Supporting strategic success through enterprise-wide reputation risk management. *Journal of Risk Finance, 17,* 26-45. doi:10.1111/jori.12065

Gaya, H. J., & Smith, E. E. (2016). Developing a qualitative single case study in the strategic management realm: An appropriate research design. *International Journal of Business Management and Economic Research*, *7*, 529-538. http://www.ijbmer.com/docs/volumes/vol7issue2/ijbmer2016070201.pdf

Gehman, J., Glaser, V. L., Eisenhardt, K. M., Gioia, D., Langley, A., & Corley, K. G. (2018). Finding theory–method fit: A comparison of three qualitative approaches to theory building. *Journal of Management Inquiry*, *27*, 284-300. doi:10.1177/1056492617706029

Gentles, S. J., Charles, C., Ploeg, J., & McKibbon, K. (2015). Sampling in qualitative research: Insights from an overview of the methods literature. *Qualitative Report, 20*, 1772-1789. doi:10.1108/TQR-2014-0045

George, A. L. (2019). Case studies and theory development: The method of structured, focused comparison. In A. L. George (Ed). *A pioneer in political and social sciences*, *3,* 191-214. doi:10.1007/978-3-319-90772-7-10

Gergen, K. J., Josselson, R., & Freeman, M. (2015). The promises of qualitative inquiry. *American Psychologist*, *70*, 7-21. doi:10.1108/AP-2015-00137-001

Ghazvini, A., & Shukur, Z. (2016). Awareness training transfer and information security content development for healthcare industry. *International Journal of Advanced Computer Science and Applications*, 7, 361-370. doi:10.1145/3168390.3168397

Giorgi, A., Giorgi, B., & Morley, J. (2017). The descriptive phenomenological psychological method. In: Willig, C. and Stainton Rogers, W., Eds., *The Sage handbook of qualitative research in psychology*, 2nd Edition, Sage, Thousand Oaks, 176-192. doi:10.4135/9781526405555.n11

Glinz, M., & Fricker, S. A. (2015). On shared understanding in software engineering: An essay. *Computer Science-Research and Development*, *30*, 363-376. doi:10.1007/s00450-014-0256-x

Goel, J. N., & Mehtre, B. M. (2015). Vulnerability assessment & penetration testing as a cyber defence technology. *Procedia Computer Science*, *57*, 710-715. doi:10.1016/j.procs.2015.07.458

Goode, S., Hoehle, H., Venkatesh, V., & Brown, S. A. (2017). User compensation as a data breach recovery action: An investigation of the Sony PlayStation network breach. *MIS Quarterly*, *41*, 703-727.

Goran, I. (2017). Cyber security risks in public high schools. Retrieved from https://academicworks.cuny.edu/cgi/viewcontent.cgi?article=1002&context=jj_etds

Goyal, D. (2016). Survey on BitLocker techniques. *International Journal of Advanced Research in Computer Science*, *7*(6), 255-257. doi:10.26483/ijarcs.v7i6.2774

Grady, C. (2018). Ethical principles in clinical research. *Principles and practice of clinical research* (pp. 19-31). Academic Press.

Graham, A., Powell, M. A., & Taylor, N. (2015). Ethical research involving children: Encouraging reflexive engagement in research with children and young people. *Children & Society, 29*, 331-343. doi:10.1111/chso.12089

Graneheim, U. H., Lindgren, B. M., & Lundman, B. (2017). Methodological challenges in qualitative content analysis: A discussion paper. *Nurse Education Today*, *56*, 29-34.

Grenier, R. S., & Dudzinska-Przesmitzki, D. (2015). A conceptual model for eliciting mental models using a composite methodology. *Human Resource Development Review*, *14*, 163-184. doi:10.1177/1534484315575966

Grover, R., Emmitt, S., & Copping, A. (2017). The typological learning framework: The application of structured precedent design knowledge in the architectural design studio. *International Journal of Technology and Design Education*, *4*, 1-20. doi:10.1007/s10798-017-9421-4

GSA-IT. (2020). IT Security procedural Guide: Media Protection (MP) CIO-IT Security-06-32, Revision 5. *U.S. General Services Administration.* Retrieved from https://www.gsa.gov/cdnstatic/Media_Protection_(MP)_%5BCIO_IT_Security_06-32_Rev_5%5D_03-27-2020.pdf

Guetterman, T. (2015). Descriptions of sampling practices within five approaches to qualitative research in education and the health sciences. *Forum Qualitative Sozial Forschung, 16*, 1-23. http://www.qualitative-research.net/index.php/fqs/article/view/2290/3826

Gunawan, J. (2015). Ensuring trustworthiness in qualitative research. *Belitung Nursing Journal*, *1*, 10-11. http://belitungraya.org/BRP/index.php/bnj

Gupta, B. B., Arachchilage, N. A., & Psannis, K. E. (2018). Defending against phishing attacks: Taxonomy of methods, current issues and future directions. *Telecommunication Systems*, *67*, 247-267.

Gustafsson, J. (2017). Single case studies vs. multiple case studies: A comparative study. http://www.diva-portal.org/smash/get/diva2:1064378/FULLTEXT01.pdf

Hadi, M. A., & Closs, S. J. (2016). Ensuring rigour and trustworthiness of qualitative research in clinical pharmacy. *International Journal of Clinical Pharmacy*, *38,* 641-646. doi:10.1007/s11096-015-0237-6

Halaseh, R. A., & Alqatawna, J. (2016). Analyzing cybercrimes strategies: The case of phishing attack. *2016 Cybersecurity and Cyberforensics Conference (CCC).* doi:10.1109/ccc.2016.25

Hall, W., Schmader, T., Aday, A., & Croft, E. (2019). Decoding the dynamics of social identity threat in the workplace: a within-person analysis of women's and men's interactions in STEM. *Social Psychological and Personality Science*, *10*(4), 542-552. doi:10.1177/1948550618772582

Hammersley, M. (2018). What is ethnography? Can it survive? Should it? *Ethnography and Education*, *13*, 1-17. doi:10.1080/17457823.2017.1298458

Harchol, Y., Abraham, I., & Pinkas, B. (2018, July). Distributed SSH key management with proactive RSA threshold signatures. In *International Conference on Applied Cryptography and Network Security* (pp. 22-43). Springer.

Harris, A. (2018). Hackers stole info on Florida teachers and students 2 years ago. They just found out. *Miami Herald.* Retrieved from https://www.miamiherald.com/news/local/education/article204464984.html#storylink=cpy

Harrison, H., Birks, M., Franklin, R., & Mills, J. (2017). Case study research: Foundations and methodological orientations. *Forum Qualitative Sozialforschung, 18*, 1-17. doi:10.17169/fqs-18.1.2655

Harvey, L. (2015). Beyond member-checking: A dialogic approach to the research interview. *International Journal of Research & Method in Education, 38*, 23-38. doi:10.3402/qhw.v9.23606

Hashemnezhad, H. (2015). Qualitative content analysis research: A review article. *Journal of ELT and Applied Linguistics*, *3*, 54-62. http://www.jeltal.com/yahoo_site_admin/ assets/docs/5.7151855.pdf

Hassanzadeh, A., Modi, S., & Mulchandani, S. (2015). Towards effective security control assignment in the Industrial Internet of Things. In *2015 IEEE 2nd World Forum on internet of Things (WF-IoT)* (pp. 795-800). IEEE.

Hayhurst, C. (2018). Sewing up solutions: The role of software patch management in effective cybersecurity. *Biomedical Instrumentation & Technology*, *52*(2), 92-102. doi:10.2345/0899-8205-52.2.92

He, W., Kshirsagar, A., Nwala, A., & Li, Y. (2019). Teaching information security with workflow technology—A case study approach. *Journal of Information Systems Education*, *25*(3), 201-210. http://jise.org/Volume25/n3/JISEv25n3p201.pdf

Heale, R., & Twycross, A. (2015). Validity and reliability in quantitative studies. *Evidence-based nursing, 18*(3), 66-67. doi:10.1136/eb-2015-102129

Hendre, A., & Joshi, K. P. (2015, June). A semantic approach to cloud security and compliance. In *2015 IEEE 8th International Conference on Cloud Computing* (pp. 1081-1084). IEEE.

Herold, B. (2017). Schools struggle to keep pace with hackings, other cyber threats. New survey data show IT leaders underestimate cybersecurity challenges. Retrieved from https://www.edweek.org/ew/articles/2017/11/29/schools-struggle-to-keep-pace-with-hackings.html

Hess, A. (2017). *Department of Education: Hackers are now targeting elementary and high schools.* Retrieved from https://www.cnbc.com

Hesse-Biber, S. (2016). Sex roles. Qualitative or mixed methods research inquiry approaches: Some loose guidelines for publishing in sex roles. *Journal of International Research, 74*(4), 1-2. doi:10.1007/s11199-015-0568-8

Hettiarachchi, S., & Wickramasinghe, S. (2016). *Study to identify threats to information systems in organizations and possible countermeasures through policy decisions and awareness programs to ensure the information security.* Retrieved from https://www.researchgate.net/profile/Samanthi_Wickramsinghe/publication/307107552_Study_to_identify_threats_to_Information_Systems_in_organizations_and possible_countermeasures_through_policy_decisions_and_awareness_programs_to_ensure_the_information_security_LIMITATION/links/57c199d308aed246b0fe011c.pdf

Hewitt, B., Dolezel, D., & McLeod, A. (2017). Mobile device security: Perspectives of future healthcare workers. *Perspectives in Health Information Management, 7*(5), 1-14. doi:10.1108/ij-05-2016-0045

Ho, A. (2017). Advancing educational research and student privacy in the “big data” era. *Workshop on Big Data in Education: Balancing the Benefits of Educational Research and Student Privacy* (pp. 1-18). National Academy of Education.

Hoffmann, R., Kiedrowicz, M., & Stanik, J. (2016). Risk management system as the basic paradigm of the information security management system in an organization. In *MATEC Web of Conferences* (Vol. 76, p. 04010). EDP Sciences. doi:10.1051/matecconf/2016760

Holtfreter, R. E., & Harrington, A. (2015). Data breach trends in the United States. *Journal of Financial Crime, 22*, 242-260. doi:10.1108/JFC-09-2013-0055

Hopkins, R. M., Regehr, G., & Pratt, D. D. (2017). A framework for negotiating positionality in phenomenological research. *Medical Teacher, 39*, 20-25. doi:10.1080/0142159X.2017.1245854

Höst, M., Sönnerup, J., Hell, M., & Olsson, T. (2018). Industrial practices in security vulnerability management for iot systems–an interview study. In *Proceedings of the International Conference on Software Engineering Research and Practice (SERP)* (pp. 61-67). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

Houghton, C., Casey, D., Shaw, D., & Murphy, K. (2013). Rigour in qualitative case study research. *Nurse Researcher, 20*, 12. doi:10.7748/nr2013.03.20.4.12.e326

Huda, M., Maseleno, A., Shahrill, M., Jasmi, K. A., Mustari, I., & Basiron, B. (2017). Exploring adaptive teaching competencies in big data era. *International Journal of Emerging Technologies in Learning*, *12*(03), 68-83. doi:10.3991/ijet.v12i03.6434

Hussein, A. (2015). The use of triangulation in social sciences research: Can qualitative and quantitative methods be combined? *Journal of Comparative Social Work, 4*. doi:10.1039/C4CS00395K

Hyland, K. (2016). Methods and methodologies in second language writing research. *System*, *59*, 116-125. doi:10.1016/j.jslw.2016.09.003

Ibrahim, A. B., & Kant, S. (2018). Penetration testing using SQL injection to recognize the vulnerable point on web pages. *International Journal of Applied Engineering Research*, *13*, 5935-5942. http://ripublication.com/ijaer18/ijaerv13n8_48.pdf

Ibrahim, N., & Edgley, A. (2015). Embedding researcher's reflexive accounts within the analysis of a semi-structured qualitative interview. *Qualitative Report*, *20*, 1671-1681. http://nsuworks.nova.edu/tqr/vol20/iss10/9

Identity Theft Resource Center. (2018). *2018 breach report.* Retrieved from https://www.idtheftcenter.org/2018-data-breaches/

Identity Theft Resource Center. (2020). *Data breaches.* Retrieved from https://www.idtheftcenter.org/data-breaches/

Iqbal, S., Mat Kiah, M. L., Dhaghighi, B., Hussain, M., Khan, S., Khan, M. K., & Raymond Choo, K. (2016). On cloud security attacks: A taxonomy and intrusion detection and prevention as a service. *Journal of Network and Computer Applications, 74*, 98-120. doi:10.1016/j.jnca.2016.08.016

Jackman, S. D., Mozgacheva, T., Chen, S., O'Huiginn, B., Bailey, L., Birol, I., & Jones, S. J. (2019). ORCA: a comprehensive bioinformatics container environment for education and research. *Bioinformatics, 35*(21), 4448-4450. doi:10.1093/bioinformatics/btz278

Jacobs, J., Romanosky, S., Adjerid, I., & Baker, W. (2019). Improving vulnerability remediation through better exploit prediction. In *2019 Workshop on the Economics of Information Security*.

Jain, J., & Pal, P. R. (2017). Detecting worms based on data mining classification technique. *International Journal of Engineering Science, 7*, 11388-11391. http://www.ttcenter.ir/ArticleFiles/ENARTICLE/3611.pdf

Jansen, J., & van Schaik, P. (2017). Comparing three models to explain precautionary online behavioural intentions. *Information & Computer Security, 25*, 165-180. doi:10.1016/j.chb.2017.05.038

Jayatilleke, S., & Lai, R. (2018). A systematic review of requirements change management. *Information and Software Technology, 93*, 163-185. doi:10.1016/j.infsof.2017.09.004

Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems, 34*(2), 597-626. doi:10.1080/07421222.2017.1334499

Johnson, M. E., Kondo, K. K., Brems, C., Ironside, E. F., & Eldridge, G. D. (2016). Mental health research in correctional settings: Perceptions of risk and vulnerabilities. *Ethics & Behavior, 26*, 238-251. doi:10.1080/10508422.2015.1011327

Johnsrud, K. (2016). *The challenges of performing it security preparedness exercises in organizations* (Master's thesis). Retrieved from https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/2388276/14163_FULLTEXT.pdf?sequence=1

Johnston, M. P. (2017). Secondary data analysis: A method of which the time has come. *Qualitative and Quantitative Methods in Libraries, 3,* 619-626. http://www.qqml-journal.net/index.php/qqml/article/download/169/170

Josey, R. (2016). The Thebes Group. What is configuration management and what we can learn from a fridge freezer? Retrieved from https://www.axelos.com/news/blogs/november-2016/what-is-configuration-management

Joslin, R., & Müller, R. (2016). Identifying interesting project phenomena using philosophical and methodological triangulation. *International Journal of Project Management, 34,* 1043-1056. doi:10.1016/j.ijproman.2016.05.005

Joyce, M. (2015). Using narrative in nursing research. *Nursing Standard. 29,* 36-41. doi:10.1108/NS-04-2014-0001

Kaghazgaran, P., & Takabi, H. (2015). Toward an insider threat detection framework using honey permissions. *Journal of internet Services and Information Security*, *5*(3), 19-36. doi:10.1016/j.cell.2015.05.007

Kalaiprasath, R., Elankavi, R., & Udayakumar, D. R. (2017). Cloud security and compliance: A semantic approach in end to end security. *International Journal of Mechanical Engineering and Technology*, *8*, 987-994. doi:10.21307/ijssis-2017-265

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*, 2954-2965. doi:10.1111/jan.13031

Kashefi, A., Nuhu, K., Abbott, P., Ayoung, D., & Alwzinani, F. (2018). Investigating users' IT adaptation behaviors: A case of a computerized work system. Retrieved from https://bura.brunel.ac.uk/bitstream/2438/17190/1/FullText.pdf

Katz, J. (2015). A theory of qualitative methodology: The social system of analytic fieldwork. *Méthod(e)s: African Review of Social Sciences Methodology*, *1*, 131-146.

Keys, B., & Shapiro, S. (2019). Frameworks and Best Practices. In *Cyber Resilience of Systems and Networks* (pp. 69-92). Springer. doi:10.1007/978-3-319-77492-3_4

Khan, F. S., Kim, J. H., Moore, R. L., & Mathiassen, L. (2019). Data breach risks and resolutions: A literature synthesis. Retrieved from https://pdfs.semanticscholar.org/d0c6/c7992769796f87a43bdbea77beae48bd27fd.pdf

Khan, K., Azam, F., Anwar, M. W., & Kiran, A. (2019, August 23). A Meta-model For Software Project Change and Configuration Management. In *Proceedings of the 9th International Conference on Information Communication and Management, Prague Czech Republic* (pp. 12-16). doi:10.1145/3357419.3357437

Khan, K., & Goodridge, W. (2019). A survey of network-based security attacks. *International Journal of Advanced Networking and Applications, 10,* 3981-3989. doi:10.35444/IJANA.2019.10051

Khou, S., Mailloux, L. O., & Pecarina, J. M. (2017). System-agnostic security domains for understanding and prioritizing systems security engineering efforts. *IEEE Access*, *5,* 3465-3474. doi:10.1109/ACCESS.2017.2670781

King, D. S. (2016). Re: Petition to Amend 34 CFR Part 99 ("Family Educational Rights and Privacy") to Establish a Data Security Rule. Retrieved from https://epic.org/privacy/student/ED-Data-Security-Petition.pdf

Kirichenko, L., Radivilova, T., & Carlsson, A. (2018). Detecting cyber threats through social network analysis: Short survey. 20-34. doi:10.21272/sec.2017.1-03

Kitchin, R., & Dodge, M. (2019). The (in)security of smart cities: Vulnerabilities, risks, mitigation, and prevention. *Journal of Urban Technology*, *26*(2), 47-65. doi:10.1080/10630732.2017.1408002

Klein, H. J. (1989). An integrated control theory model of work motivation. *Academy of Management Review*, *14*, 150-172. doi:10.1177/ 1989-20515-001

Ko, A. J., Latoza, T. D., & Burnett, M. M. (2015). A practical guide to controlled experiments of software engineering tools with human participants. *Empirical Software Engineering*, *20*, 110-141. doi:10.1007/s10664-013-9279-3

Kongnso, F. J. (2015). *Best practices to minimize data security breaches for increased business performance* [Doctoral dissertation, Walden University]. ScholarWorks. Retrieved from https://scholarworks.waldenu.edu

Kornbluh, M. (2015). Combatting challenges to establishing trustworthiness in qualitative research. *Qualitative Research in Psychology*, *12*, 397-414.

Kostopoulos, G., Rizomyliotis, I., & Konstantoulaki, K. (2015). Determinants of physicians' purchase intention for innovative services: Integrating professional characteristics with technology acceptance model and theory of planned behaviour. *International Journal of Innovation Management*, *19*(02), 1550024. doi:10.1142/S1363919615500243

Kressin, J. (2019). Cyber attacks in schools: It CAN happen to your district. Retrieved from https://blog.identityautomation.com/cyber-attacks-in-schools-it-can-happen-to-your-district

Kristadi, D., & Sucahyo, Y. G. (2016). Factors analysis of IPv6 user acceptance against security aspects based on concept of technology acceptance model (TAM) and technology threat avoidance theory (TTAT). *International Conference on Advanced Computer Science and Information Systems*, *5,* 67-72. doi:10.1109/ICACSIS.2016.7872750

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, *22*, 113-122. doi:10.1016/j.jisa.2014.09.005

Krosnick, J. A. (2018). Questionnaire design. In *The Palgrave handbook of survey research* (pp. 439-455). Palgrave Macmillan. doi:10.1007/978-3-319-54395-6_53

Kumar, P., & Kumar, R. (2016). Cyber security's significance in health information technology (HIT). *International Journal of Advanced Studies in Computers, Science and Engineering*, *5*(2), 8-25. doi:10.1007/s00134-017-4683-6

Kumar, S. A., Vealey, T., & Srivastava, H. (2016, January). Security in internet of things: Challenges, solutions and future directions. *49th Hawaii International Conference on System Sciences (HICSS)* (pp. 5772-5781). IEEE.

Kumar, S. N. (2015). Review on network security and cryptography. *International Transaction of Electrical and Computer Engineers System*, *3*, 1-11. http://faratarjome.ir/u/media/shopping_files/store-EN-1485601568-926.pdf

Kuypers, M. A., Maillart, T., & Pate-Cornell, E. (2016). An empirical analysis of cyber security incidents at a large organization. http://fsi.stanford.edu/sites/default/files/kuypersweis_v7.pdf

Lal, S., Taleb, T., & Dutta, A. (2017). NFV: Security threats and best practices. *IEEE Communications Magazine*, *55*(8), 211-217. doi:10.1109/MCOM.2017.1600899

Lancaster, K. (2017). Confidentiality, anonymity and power relations in elite interviewing: conducting qualitative policy research in a politicised domain. *International Journal of Social Research Methodology, 20*(1), 93-103. doi:10.1080/13645579.2015.1123555

Leung, L. (2015). Validity, reliability, and generalizability in qualitative research. *Journal of Family Medicine and Primary Care*, *4,* 324-344. doi:10.4103/2249-4863.161306

Levin, D. A. (2020). The state of K-12 cybersecurity: 2019 year in review. Arlington, VA: EdTech Strategies.

Lewis, N., Campbell, M. J., & Baskin, C. R. (2015). Information security for compliance with select agent regulations. *Health Security, 13*, 207-218. doi:10.1089/hs.2014.0090

Lewis, S. (2015). Qualitative inquiry and research design: Choosing among five approaches. *Health Promotion Practice*, *16*, 473-475. doi:10.4103/2249-4863.161306

Lewis, S. G., & Palumbo, T. (2018, September 11). BitLocker Full-Disk Encryption: Four Years Later. In *Proceedings of the 2018 ACM SIGUCCS Annual Conference,* ACM, New York, NY, USA, 147-150. doi:10.1145/3235715.3241363

Li, F., Rogers, L., Mathur, A., Malkin, N., & Chetty, M. (2019, August 12). Keepers of the machines: examining how system administrators manage software updates. In *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security* (pp. 273-288). Berkeley, CA, USA, 2019. USENIX Association

Li, S., Tryfonas, T., & Li, H. (2016). The internet of things: A security point of view. *Internet Research, 26*, 337-359. doi:10.1108/IntR-07-2014-0173

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly, 33*, 71-90. doi:10.2307/20650279

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, *11*(7), 394-413. doi:10.2307/20650279

Loukaka, A., & Rahman, S. (2017). Discovering new cyber protection approaches from a security professional prospective. *International Journal of Computer Networks & Communications*, *9*(4). doi:10.5121/ijcnc.2017.9402

Lub, V. (2015). Validity in qualitative evaluation: Linking purposes, paradigms, and perspectives. *International Journal of Qualitative Methods, 14*, 1–8. doi:10.1177/1609406915621406

Machado, L. J., & Chung, C. J. (2015). Integrating technology: The principals' role and effect. *International Education Studies*, *8*(5), 43-53. doi:10.5539/ies.v8n5p43

Maher, C., Hadfield, M., Hutchings, M., & de Eyto, A. (2018). Ensuring rigor in qualitative data analysis: A design research approach to coding combining NVivo with traditional material methods. *International Journal of Qualitative Methods, 17*, 1609406918786362. doi:10.1177/1609406918786362

Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R. P., & Ni, W. (2018). Anatomy of threats to the internet of Things. *IEEE Communications Surveys & Tutorials*, *21*(2), 1636-1675. doi:10.1109/COMST.2018.2874978

Malterud, K., Siersma, V. D., & Guassora, A. D. (2016). Sample size in qualitative interview studies: Guided by information power. *Qualitative Health Research*, *26*, 1753-1760.

Markus, M. L., & Robey, D. (1988). Information technology and organizational change: causal structure in theory and research. *Management Science*, *34*(5), 583-598. doi:10.1287/mnsc.34.5.583

Martin, K. (2017, December 8). Data breach exposes social security numbers, birth dates of hundreds of Texas students. *The Dallas News.* Retrieved from https://www.dallasnews.com/news/education/2017/12/08/data-breach-exposes-social-security-numbers-birth-dates-of-hundreds-of-texas-students/

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, *81*, 36-58. doi:10.1509/jm.15.0497

Maxwell, S. E., Lau, M. Y., & Howard, G. S. (2015). Is psychology suffering from a replication crisis? What does “failure to replicate” really mean? *American Psychologist*, *70*, 487-490. doi:10.1509/jm.15.0497

Mayer, N., Aubert, J., Grandry, E., Feltus, C., Goettelmann, E., & Wieringa, R. (2019). An integrated conceptual model for information system security risk management supported by enterprise architecture management. *Software & Systems Modeling*, *18*, 2285-2312. doi:10.1007/s10270-018-0661-x

Mayoh, J., & Onwuegbuzie, A. J. (2015). Toward a conceptualization of mixed methods phenomenological research. *Journal of Mixed Methods Research*, *9*, 91-107. doi:10.1177/1558689813505358

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

McKnight, K., O'Malley, K., Ruzic, R., Horsley, M. K., Franey, J. J., & Bassett, K. (2016). Teaching in a digital age: How educators use technology to improve student learning. *Journal of Research on Technology in Education*, *48*(3), 194-211. doi:10.1080/15391523.2016.1175856

Meijer, C., & Van Gastel, B. (2019, May 19). Self-encrypting deception: weaknesses in the encryption of solid state drives. In *2019 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, 2019, pp. 72-87.

Mihalos, M. G., Nalmpantis, S. I., & Ovaliadis, K. (2019). Design and Implementation of Firewall Security Policies using Linux Iptables. *Journal of Engineering Science & Technology Review*, *12*(1), 80-86. doi:10.25103/jestr.121.09

Miracle, V. A. (2016). The Belmont report: The triple crown of research ethics. *Dimensions of Critical Care Nursing*, *35*, 223-228. doi:10.1097/DCC.0000000000000186

Mishra, D., Goel, V., & Virbahu Jain, I. J. E. R. T. (2017). *Security or breach—Enterprise to decide.* Retrieved from https://www.ijert.org/browse

Mishra, S. (2015). Organizational objectives for information security governance: A value focused assessment. *Information & Computer Security*, *23*, 122-144. doi:10.1108/ICS-02-2014-0016

Mitra, S., Guzman, I. R., Dhillon, G., & Tran, K. (2016). *A quantitative investigation of the security factors affecting the use of IT systems in public networks.* http://029e2c6.netsolhost.com/II-Proceedings/2014/IIVC_2014_submission_2.docx

Mohajan, H. K. (2018). Qualitative research methodology in social sciences and related subjects. *Journal of Economic Development, Environment and People*, *7*, 23-48. doi:10.26458/jedep.v7i1.571

Mohammad, H., Hassan, P. F., & Yaman, S. K. (2017). A qualitative content analysis on technical competency for Malaysian construction managers. *Pertanika Journal of Social Sciences and Humanities, 25*, 341-356. doi:10.1051/matecconf/201710303012

Montano, D. E., & Kasprzyk, D. (2015). Theory of reasoned action, theory of planned behavior, and the integrated behavioral model. *Health Behavior: Theory, Research and Practice*, *70*(4), 231-256. http://www.ssu.ac.ir/cms/fileadmin/user_upload/Daneshkadaha/dbehdasht/Asadeghi/kar_dar_khane/1._Karen_Glanz__Barbara_K._Rimer__K._Viswanath__Heal_BookFi.org__.pdf#page=105

Montgomery, D. (2018, February 2). How rampant are cyberattacks in Texas? Fort Worth defends about 15,000 threats daily. *Fort Worth Star-Telegram.* Retrieved from https://www.star-telegram.com/news/local/fort-worth/article198030174.html

Morozov, V., Kalnichenko, O., Timinsky, A., & Liubyma, I. (2017, September). Projects change management in based on the projects configuration management for developing complex projects. In *2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)* (Vol. 2, pp. 939-941). IEEE. doi:10.1109/IDAACS.2017.8095224

Morse, J. M. (2015). Critical analysis of strategies for determining rigor in qualitative inquiry. *Qualitative Health Research, 25*, 1212-1222. doi:10.1177/1049732315588501

Morse, J. M., & Coulehan, J. (2015). Maintaining confidentiality in qualitative publications. *Qualitative Health Research, 25*, 151-152. doi:10.1177/1049732314563489

Mortari, L. (2015). Reflectivity in research practice. *International Journal of Qualitative Methods, 14*, 160940691561804. doi:10.1177/1609406915618045

Mozumder, D. P., Mahi, M. N., Whaiduzzaman, M., & Mahi, M. J. N. (2017). Cloud computing security breaches and threats analysis. *International Journal of Scientific & Engineering Research*, *8*, 1287-1297. doi:10.1108/ISER-2016-0012

Mungekar, A., Solanki, Y., & Swarnalatha, R. (2020). Augmentation of a SCADA based firewall against foreign hacking devices. *International Journal of Electrical & Computer Engineering*, *10*(2), 1359-1366. doi:10.11591/ijece.v10i2.pp1359-1366

Murdock, D. (2018). *Promoting growth and self-efficacy: A phenomenological study of the lived experiences of first-year assistant principals* (Doctoral dissertation, Kennesaw State University in Georgia). Kennesaw State University Digital

Archive. Retrieved from https://digitalcommons.kennesaw.edu/educleaddoc_etd/15

Mushtaq, M. F., Akram, U., Khan, I., Khan, S. N., Shahzad, A., & Ullah, A. (2017). Cloud computing environment and security challenges: A review. *International Journal of Advanced Computer Science and Application*, *8*(10), 183-195.

Nashwan, S., & Alshammari, B. (2017). Formal analysis of MCAP protocol against replay attack. *British Journal of Mathematics & Computer Science*, *22*, 1-14. doi:10.9734/BJMCS/2017/32744

Nasir, A., Arshah, R. A., Ab Hamid, M. R., & Fahmy, S. (2019). An analysis on the dimensions of information security culture concept: A review. *Journal of Information Security and Applications*, *44*, 12-22. doi:10.1016/j.jisa.2018.11.003

National School Boards Association. (2017). *Data security for schools. A legal and policy guide for school boards.* Retrieved from https://cdn-files.nsba.org/s3fs-public/reports/Data_Security_Guide_5_Jan2017.pdf?G4UaLHlwi3zo6iSq94F.K.vSAaCmzb.y

Neal, J. W., Neal, Z. P., VanDyke, E., & Kornbluh, M. (2015). Expediting the analysis of qualitative data in evaluation: A procedure for the rapid identification of themes from audio recordings (RITA). *American Journal of Evaluation*, *36*, 118-132. doi:10.1177/1098214014536601

Neale, J. (2016). Iterative categorization (IC): a systematic technique for analysing qualitative data. *Addiction*, *111*, 1096-1106. doi:10.1111/add.13314

Nebeker, C., Linares-Orozco, R., & Crist, K. (2015). A multi-case study of research using mobile imaging, sensing and tracking technologies to objectively measure behavior: Ethical issues and insights to guide responsible research practice. *Journal of Research Administration*, *46*, 118-137. doi:10.1008/JRA-2014-0012

Newcomer, K. E., Hatry, H. P., & Wholey, J. S. (2015). Conducting semi-structured interviews. *Handbook of practical program evaluation*, *492-504*. doi:10.1002/9781119171386

Nguyen, Q., Ghosh, P., & Krishnamachari, B. (2018, March). End-to-end network performance monitoring for dispersed computing. *2018 International Conference on Computing, Networking and Communications (ICNC)* (pp. 707-711). IEEE.

Nkenyereye, L., & Jang, J. W. (2017). Design of environmental monitoring system for auxiliary data center using lower hardware cost. *International Journal of Control and Automation*, *10*(2), 89-102. doi:10.14257/ijca.2017.10.2.08

Noble, H., & Smith, J. (2015). Issues of validity and reliability in qualitative research. *Evidence Based Nursing*, *18*(2), 34-35. doi:10.1136/eb-2015-102054

Noguerol, L. O., & Branch, R. (2018). Leadership and electronic data security within small businesses: An exploratory case study. *Journal of Economic Development, Management, IT, Finance, and Marketing*, *10*(2), 7-35. Retrieved from https://gsmi-ijgb.com

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods*, *16*, 160940691773384. doi:10.1177/1609406917733847

Nullah, N. (2018). The influence of the pyramid discussion towards the student writing ability. *Journal of Languages and Language Teaching*, *4*(2), 74-78. doi:10.33394/jollt.v4i2.322

Obenchain, K., & Ives, B. (2015). Subjects or participants? The development of ethical principles in research involving humans in the United States. *Psihologia Resurselor Umane*, *5*, 105-107. http://www.apio.ro/pru/

O'Boyle, E. H., Banks, G. C., & Gonzalez-Mulé, E. (2017). The chrysalis effect: How ugly initial results metamorphosize into beautiful articles. *Journal of Management*, *43*, 376-399. doi:10.1177/0149206314527133

Odelu, V., Das, A. K., & Goswami, A. (2015). A secure biometrics-based multi-server authentication protocol using smart cards. *IEEE Transactions on Information Forensics and Security*, *10*, 1953-1966. doi:10.1109/TIFS.2015.2439964

Ogbonna, L. (2020). *Technical strategies database managers use to protect systems from security breaches* [Doctoral dissertation, Walden University). Retrieved from https://scholarworks.waldenu.edu

Oh, S., Kim, E., Jeong, J., Ko, H., & Kim, H. (2017, January 5). A flexible architecture for orchestrating network security functions to support high-level security policies. In *Proceedings of the 11th International Conference on Ubiquitous Information Management and Communication,* Beppu Japan (pp. 1-5). doi:10.1145/3022227.3022270

Oktarina, N., & Pramusinto, H. (2016). School accountability model based on archive. *International Conference on Education for Economics, Business, and Finance*, *6,* 260-267. http://iceebf.um.ac.id/

Oltmann, S. M. (2016). Qualitative interviews: A methodological discussion of the interviewer and respondent contexts. *Forum: Qualitative Social Research*, *17,* 88-102. doi:10.17169/fqs-17.2.2551

Olusolade Aribake, F., & Mat Aji, Z. (2020). Modelling the phishing avoidance behaviour among internet banking users in Nigeria: The initial investigation. *Journal of Computer Engineering and Technology*, *4*(1), 1-17. Retrieved from https://ssrn.com/abstract=3528954

Onwuegbuzie, A. J., & Byers, V. T. (2014). An exemplar for combining the collection, analysis, and interpretation of verbal and nonverbal data in qualitative research. *International Journal of Education*, *6*, 183-246. doi:10.5296/ije.v6i14399

O.Nyumba, T., Wilson, K., Derrick, C. J., & Mukherjee, N. (2018). The use of focus group discussion methodology: Insights from two decades of application in conservation. *Methods in Ecology and Evolution, 9*, 20-32. doi:10.1111/2041-210x.12860

Osanloo, A., & Grant, C. (2016). Understanding, selecting, and integrating a theoretical framework in dissertation research: Creating the blueprint for your “house”. *Administrative Issues Journal: Connecting Education, Practice, and Research*, *4*(2), 7-23. doi:10.5929/2014.4.2.9

Pacho, T. (2015). Exploring participants’ experiences using case study. *International Journal of Humanities and Social Science*, *5*(4), 44-53.

Paine, G. (2015). A pattern-generating tool for use in semi-structured interviews. *Qualitative Report*, *20*, 468-481. Retrieved from https://nsuworks.nova.edu/tqr

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health and Mental Health Services Research*, *42*, 533-544. doi:10.1007/s10488-013-0528-y

Park, K. O. (2018). The relationship between BPR strategy and change management for the sustainable implementation of ERP: An information orientation perspective. *Sustainability*, *10*(9), 3080. doi:10.3390/su10093080

Park, N. K., Chun, M. Y., & Lee, J. (2016). Revisiting individual creativity assessment: Triangulation in subjective and objective assessment methods. *Creativity Research Journal*, *28*, 1-10. doi:10.1080/10400419.2016.1125259

Patel, M. (2020). *Demilitarized zone: An exceptional layer of network security to mitigate DDoS attack* [Doctoral dissertation, University of Windsor, Canada]. University of Windsor Digital Archive. Retrieved from https://scholar.uwindsor.ca/cgi/viewcontent.cgi?article=9311&context=etd

Pathak, A., & Intratat, C. (2016). Use of semi-structured interviews to investigate teacher perceptions of student collaboration. *Malaysian Journal of ELT Research*, *8*, 10-22. http://www.melta.org.my

Pawlowski, S. D., & Jung, Y. (2015). Social representations of cybersecurity by university students and implications for instructional design. *Journal of Information Systems Education*, *26*, 281-294. doi:10.1108/JISE-2014-0014

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

Pereira, T., Barreto, L., & Amaral, A. (2017). Network and information security challenges within Industry 4.0 paradigm. *Procedia Manufacturing*, *13*, 1253-1260. doi:10.1016/j.promfg.2017.09.047

Perkmann, M., & Schildt, H. (2015). Open data partnerships between firms and universities: The role of boundary organizations. *Research Policy*, *44*, 1133-1143. doi:10.1016/j.respol.2014.12.006

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

Plachkinova, M., & Maurer, C. (2019). Security breach at target. *Journal of Information Systems Education*, *29*, 7-16. http://jise.org/Volume29/n1/JISEv29n1p11.pdf

Ponelis, S. R. (2015). Using interpretive qualitative case studies for exploratory research in doctoral studies: A case of information systems research in small and medium enterprises. *International Journal of Doctoral Studies*, *10*, 535-550. doi:10.28945/2339

Ponemon Institute. (2019). Cost of a data breach report: Global analysis. Retrieved from https://www.ibm.com/security/data-breach

Popping, R. (2015). Analyzing open-ended questions by means of text analysis procedures. *Bulletin of Sociological Methodology/Bulletin de Méthodologie Sociologique*, *128*, 23-39. doi:10.1177/0759106315597389

Poudyal, S., Dasgupta, D., Akhtar, Z., & Gupta, K. (2019). A multi-level ransomware detection framework using natural language processing and machine learning. *14th International Conference on Malicious and Unwanted Software (MALCON)*.

Pratt-Sensie, A. A. (2020). *Security strategies to prevent data breaches in infrastructure as a service cloud computing* [Doctoral dissertation, Walden University]. ScholarWorks. Retrieved from https://scholarworks.waldenu.edu

PricewaterhouseCoopers. (2015). *Price Water Corporation information security breaches. technical report.* http://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf

Privacy Rights Clearinghouse. (2016a). Chronology of data breaches: FAQ. Retrieved from https://www.privacyrights.org/chronology-data-breaches-faq

Privacy Rights Clearinghouse. (2016b). Data breaches. Retrieved from https://www.privacyrights.org/data-breaches

Proofpoint. (2020). Proofpoint’s state of the phish report stresses the need for user training and email reporting as targeted attacks climb. Retrieved from https://www.globenewswire.com/news-release/2020/01/23/1974287/0/en/Proofpoint-s-State-of-the-Phish-Report-Stresses-the-Need-for-User-Training-and-Email-Reporting-as-Targeted-Attacks-Climb.html

QSR International. (2019). NVivo 12 Pro Software. Retrieved from https://www.qsrinternational.com/

Queirós, A., Faria, D., & Almeida, F. (2017). Strengths and limitations of qualitative and quantitative research methods. *European Journal of Education Studies*. *3*(9), 1-19. doi:10.5281/zenodo.887089

Raja, A. (2019). *How to best mitigate cybersecurity risks and protect your data*. Retrieved from https://www.atlantic.net/hipaa-compliant-hosting/how-to-best-mitigate-cybersecurity-risks-and-protect-your-data/

Ramachandran, M., & Chang, V. (2016). Towards performance evaluation of cloud service providers for cloud data security. *International Journal of Information Management*, *36*, 618-625. doi:10.1016/j.ijinfomgt.2016.03.005

Ramalingam, R., Khan, S., & Mohammed, S. (2016, May 12-13). *The need for effective information security awareness practices in Oman higher educational institutions* [Paper presentation]. 1st Symposium on Communication, Information Technology, and Biotechnology: Current Trends and Future Scope, Sur College of Applied Sciences, Ministry of Higher education, Sultanate of Oman. Retrieved from https://arxiv.org/abs/1602.06510

Regenscheid, A., Feldman, L., & Witte, G. (2015). *NIST Special Publication 800-88 Revision 1, Guidelines for Media Sanitization*. National Institute of Standards and Technology. Retrieved from https://csrc.nist.gov/csrc

Ren, Z., Chen, C., & Zhang, L. (2018). Security protection under the environment of WiFi. *2017 International Conference Advanced Engineering and Technology Research (AETR 2017)*. Atlantis Press.

Rezaeibagha, F., Win, K. T., & Susilo, W. (2015). A systematic literature review on security and privacy of electronic health record systems: Technical perspectives. *Health Information Management Journal*, *44*(3), 23-38. doi:10.1177/183335831504400304

Robb, K. A., Gatting, L., & Wardle, J. (2017). What impact do questionnaire length and monetary incentives have on mailed health psychology survey response? *British Journal of Health Psychology*, *22*, 671-685. doi:10.1111/bjhp.12239

Rose, D. C., Brotherton, P. N., Owens, S., & Pryke, T. (2018). Honest advocacy for nature: Presenting a persuasive narrative for conservation. *Biodiversity and conservation*, *27*, 1703-1723. doi:10.3389/fmars.2017.00096/full

Rosenberg, J. M., & Koehler, M. J. (2015). Context and technological pedagogical content knowledge (TPACK): A systematic review. *Journal of Research on Technology in Education*, *47*(3), 186-210. doi:10.1080/15391523.2015.1052663

Roulston, K., & Shelton, S. A. (2015). Reconceptualizing bias in teaching qualitative research methods. *Qualitative Inquiry, 21*, 332-342. doi:10.1177/1077800414563803

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*, 65-78. doi:10.1016/j.cose.2015.05.012

Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., ... & Jinks, C. (2018). Saturation in qualitative research: Exploring its conceptualization and operationalization. *Quality & Quantity*, *52*, 1893-1907. doi:10.1007/s11135-017-0574-8

Saunders, M. N., & Townsend, K. (2016). Reporting and justifying the number of interview participants in organization and workplace research. *British Journal of Management*, *27*, 836-852. doi:10.1111/1467-8551.12182

Schmidlin, K., Clough-Gorr, K. M., & Spoerri, A. (2015). Privacy preserving probabilistic record linkage (P3RL): A novel method for linking existing health-related data and maintaining participant confidentiality. *BMC Medical Research Methodology*, *15*, 46-74. doi:10.1186/s12874-015-0038-6

Schneier, B. (2018). Internet hacking is about to get much worse: We can no longer leave online security to the market. Retrieved from https://www.schneier.com/essays/archives/2018/10/internet_hacking_is_.html

Schwab, J. R., & Syed, M. (2015). Qualitative inquiry and emerging adulthood: Meta-theoretical and methodological issues. *Emerging Adulthood*, *3*(6), 388-399. doi:10.1177/2167696815587801

Selwyn, N., & Bulfin, S. (2016). Exploring school regulation of students’ technology use–rules that are made to be broken? *Educational Review*, *68*, 274-290. doi:10.1080/00131911.2015.1090401

Semenova, N., & Hassel, L. G. (2015). On the validity of environmental performance metrics. *Journal of Business Ethics, 132*, 249-258. doi:10.1007/s10551-014-2323-4

Shackelford, S. J. (2016). Protecting intellectual property and privacy in the digital age: The use of national cybersecurity strategies to mitigate cyber risk. *Chapman Law Review, 19*, 412-445. Retrieved from https://digitalcommons.chapman.edu/cgi/viewcontent.cgi?article=1376&context=chapman-law-review

Shafiq, M., Ahmad, M., & Choi, J. G. (2017). Public system usability analysis for the valuation of cognitive burden and interface standardization: A case study of cross-ATM design. *Journal of Organizational Computing and Electronic Commerce, 27*, 162-196. doi:10.1002/cncr.21569

Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). *Computers & Security*, *57*, 14-30. doi:10.1016/j.cose.2015.11.001

Sharma, G. (2017). Pros and cons of different sampling techniques. *International Journal of Applied Research, 3*, 749-752.

Simpson, A., & Quigley, C. F. (2016). Member checking process with adolescent students: Not just reading a transcript. *Qualitative Report*, *21*, 376-392. Retrieved from https://nsuworks.nova.edu/tqr

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, 101-121. doi:10.1080/1750984X.2017.1317357

Sohail, H., & Venugopal, D. (2017). A study on the alternative strategies and approaches to condense the security challenges and threats faced in the area of cloud computing. *Journal of Student Research,* 1-4. Retrieved from https://jofsr.org/index.php/path/article/download/553/265

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*, 215-225. doi:10.1016/j.ijinfomgt.2015.11.009

Stahl, W. M., & Karger, J. (2016). Student data privacy, digital learning, and special education: Challenges at the intersection of policy and practice. *Journal of Special Education Leadership*, *29*(2), 79-88. Retrieved from https://files.eric.ed.gov/fulltext/EJ1118549.pdf

Steinbart, P. J., Keith, M. J., & Babb, J. (2016). Examining the continuance of secure behavior: A longitudinal field study of mobile device authentication. *Information Systems Research*, *27*, 219-239. doi:10.1287/isre.2016.0634

Stewart, H., Gapp, R., & Harwood, I. (2017). Exploring the alchemy of qualitative management research: Seeking trustworthiness, credibility and rigor through crystallization. *Qualitative Report*, *22*(1), 1-19. Retrieved from https://nsuworks.nova.edu/tqr

Subedi, K. P., Budhathoki, D. R., Chen, B., & Dasgupta, D. (2017, November 27). RDS3: Ransomware defense strategy by using stealthily spare space. In *2017*

IEEE Symposium Series on Computational Intelligence (SSCI) (pp. 1-8). doi:10.1109/SSCI.2017.8280842

Sugiura, L., Wiles, R., & Pope, C. (2017). Ethical challenges in online research: Public/private perceptions. *Research Ethics*, *13*(3-4), 184-199. doi:10.1177/1747016116650720

Suharyanto, C. E. (2017). Potential Threat Analysis Hypertext Transfer Protocol and Secure Hypertext Transfer Protocol of Public WiFi Users (Batam Case). *International Journal of Scientific & Engineering Research*, *8*(3), 320-326.

Taherdoost, H. (2016). Sampling methods in research methodology: How to choose a sampling technique for research. *International Journal of Advance Research in Management*, 5(2), 18-27. doi:10.1108/IJARM-2015-0014

Tarhini, A., Arachchilage, N. A. G., Masa'deh, R., & Abbasi, M. S. (2015). A critical review of theories and models of technology adoption and acceptance in information system research. *International Journal of Technology Diffusion, 6*(4), 58-77. doi:10.4018/ijtd.2015100104

Taylor, P., Dowding, D., & Johnson, M. (2017). Clinical decision making in the recognition of dying: A qualitative interview study. *BMC Palliative Care*, *16*, 1-11. doi:10.1186/s12904-016-0179-3

Taylor, T., Bedau, M., Channon, A., Ackley, D., Banzhaf, W., Beslon, G., ... & McMullin, B. (2016). Open-ended evolution: Perspectives from the OEE workshop in York. *Artificial Life*, *22*, 408-423. doi:10.1162/artl_a_00210

Taylor-Jackson, J., McAlaney, J., Foster, J., Bello, A., Maurushat, A., & Dale, J. (2020). Incorporating Psychology into Cyber Security Education: A Pedagogical Approach. *Proceedings of Asia USEC, 20*. http://www.usablesecurity.net/USEC/asiausec20/papers/AsiaUSEC20_paper_14.pdf

Teitz, L. (2017). *Personal info at risk as cyber crooks target school districts.* Retrieved from https://www.beaumontenterprise.com/news/article/Personal-info-at-risk-as-cyber-crooks-target-11063366.php

Tetnowski, J. (2015). Qualitative case study research design. *Perspectives on Fluency and Fluency Disorders, 25*, 39. doi:10.1044/ffd25.1.39

Thomas, D. R. (2017). Feedback from research participants: Are member checks useful in qualitative research? *Qualitative Research in Psychology*, *14*, 23-41.

Thomas, J. (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. *International Journal of Business Management*, *12*(3), 1-23. doi:10.5539/ijbm.v13n6p1

Thomas, J., & Galligher, G. (2018). Improving backup system evaluations in information security risk assessments to combat ransomware. *Computer and Information Science*, *11(1),* 14-25. doi:10.5539/cis.v11n1p14

Tiainen, T. (2020). Third-party software patch management in Windows environments. Retrieved from https://www.theseus.fi/bitstream/handle/10024/334222/Third%20party%20softwa re%20patch%20management%20in%20Windows%20environments2.pdf?sequence=2&isAllowed=y

Tong, A., & Dew, M. A. (2016). Qualitative research in transplantation: Ensuring relevance and rigor. *Transplantation*, *100*, 710-712. doi:10.1097/TP.0000000000001117

Tracey, S., O'Sullivan, T. L., Lane, D. E., Guy, E., & Courtemanche, J. (2017). Promoting resilience using an asset-based approach to business continuity planning. *SAGE Open, 7*(2), 215824401770671. doi:10.1177/2158244017706712

Tran, V., Porcher, R., Falissard, B., & Ravaud, P. (2016). Point of data saturation was assessed using resampling methods in a survey with open-ended questions. *Journal of Clinical Epidemiology, 80,* 88-96. doi:10.1016/j.jclinepi.2016.07.014

Tsai, H. Y. 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*, 138-150.

Tu, Z., Turel, O., Yuan, Y., & Archer, N. (2015). Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination. *Information & Management*, *52,* 506-517.

Tu, Z., Yuan, Y., & Archer, N. (2014). Understanding user behaviour in coping with security threats of mobile device loss and theft. *International Journal of Mobile Communications, 12,* 603-623. doi:10.1504/IJMC.2014.064915

Tuapawa, K. (2017). Interpreting experiences of students using educational online technologies to interact with teachers in blended tertiary environments: A phenomenological study. *Australasian Journal of Educational Technology*, *33,* 163-175. doi:10.14742/ajet.2964

Tuor, A., Kaplan, S., Hutchinson, B., Nichols, N., & Robinson, S. (2017, March). Deep learning for unsupervised insider threat detection in structured cybersecurity data streams. *Workshops at the Thirty-First AAAI Conference on Artificial Intelligence*. Retrieved from https://www.aaai.org/ocs/index.php/AAAI/AAAI17/paper/download/14228/14238

Turner, S. F., Cardinal, L. B., & Burton, R. M. (2017). Research design for mixed methods. *Organizational Research Methods*, *20*, 243-267. doi:10.1177/1094428115610808

Tweneboah-Koduah, S., & Buchanan, W. J. (2018). Security risk assessment of critical infrastructure systems: A comparative study. *Computer Journal*, *61*, 1389-1406. doi:10.1093/comjnl/bxy002

Twining, P., Heller, R. S., Nussbaum, M., & Tsai, C.-C. (2017). Some guidance on conducting and reporting qualitative studies. Computers & Education, 106, A1–A9. doi:10.1016/j.compedu.2016.12.002

U.S. Department of Education. (2017). *Data breach.* Retrieved from https://studentprivacy.ed.gov/topic/data-breach

U.S. Department of Education. (2018). *Best practices for data destruction.* Retrieved from https://studentprivacy.ed.gov

U.S. Department of Health & Human Services. (1979, April). *Ethical principles and guidelines for the protection of human subjects of research.* http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html

U.S. Environmental Protection Agency. (2019). *Information security – Media protection procedures.* Retrieved from https://www.epa.gov/sites/production/files/2016-01/documents/cio_2150-p-10.2.pdf

Valerio, M. A., Rodriguez, N., Winkler, P., Lopez, J., Dennison, M., Liang, Y., & Turner, B. J. (2016). Comparing two sampling methods to engage hard-to-reach communities in research priority setting. *BMC Medical Research Methodology, 16*, 146.

Vanhoef, M., Bhandaru, N., Derham, T., Ouzieli, I., & Piessens, F. (2018, June18). Operating channel validation: preventing Multi-Channel Man-in-the-Middle attacks against protected Wi-Fi networks. In *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks* (pp. 34-39). Stockholm, Sweden. doi:10.1145/3212480.3212493

Vaughn, P., & Turner, C. (2016). Decoding via coding: Analyzing qualitative text data through thematic coding and survey methodologies. *Journal of Library Administration, 56*, 41-51. doi:10.1080/01930826.2015.1105035

Velte, C. J., Wilfahrt, A., Müller, R., & Steinhilper, R. (2017). Complexity in a life cycle perspective. *Procedia CIRP, 61*, 104-109.

Venkatraman, S. (2017). Autonomic framework for IT security governance. *International Journal of Managing Information Technology*, *9*(3), 1-11. doi:10.5121/ijmit.2017.9301

Verizon. (2019). *Data breach investigation report.* Retrieved from https://www.verizondigitalmedia.com/blog/2017/07/2017-verizon-data-breach-investigations-report/

Victoria ISD. (2018). *Data security incident notice. Victoria Independent School District notifies public of data security incident.* Retrieved from https://www.visd.net/apps/pages/data-security-incident

Vitak, J., Shilton, K., & Ashktorab, Z. (2016, February 27). Beyond the Belmont principles: Ethical challenges, practices, and beliefs in the online data research community. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing* (pp. 941-953). New York, NY, United States. doi:10.1145/2818048.2820078

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*, 1–11. doi:10.1155/2017/2057260

Wachyudy, D. (2018). Could affectivity compete better than efficacy in describing and explaining individuals’ coping behavior: An empirical investigation. *Journal of High Technology Management Research*, *29*, 57-70. doi:10.1016/j.hitech.2018.04.006

WaldenU. (2015a). *Institutional Review Board for ethical standards in research*. http://academicguides.waldenu.edu/researchcenter/orec

WaldenU. (2015b). *IRB guidance for conducting doctoral research in your own professional setting*. http://academicguides.waldenu.edu/researchcenter/orec

WaldenU. (2015c). *Research ethics planning worksheet.* http://academicguides.waldenu.edu/researchcenter/orec

Walther, J., Sochacka, N. W., Benson, L. C., Bumbaco, A. E., Kellam, N., Pawley, A. L., & Phillips, C. M. (2017). Qualitative research quality: A collaborative inquiry across multiple methodological perspectives. *Journal of Engineering Education, 106*, 398-430.

Wamba, S. F., Akter, S., Edwards, A., Chopin, G., & Gnanzou, D. (2015). How ‘big data’ can make big impact: Findings from a systematic review and a longitudinal case study. *International Journal of Production Economics*, *165*, 234-246.

Wanyonyi, E., Rodrigues, A., Abeka, S. O., & Ogara, S. (2017). Effectiveness of security controls on electronic health records. *International Journal of Scientific & Technology Research*, *6*(12), 47-54. http://www.ijstr.org

Wash, R., Rader, E., Berman, R., & Wellmer, Z. (2016). Understanding password choices: How frequently entered passwords are re-used across websites. In *Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016)* (pp. 175-188). Denver, CO, USA.

Weishäupl, E., Yasasin, E., & Schryen, G. (2018). Information security investments: An exploratory multiple case study on decision-making, evaluation and learning. *Computers & Security*, *77*, 807-823. doi:10.1016/j.cose.2018.02.001

Wen, S. F., Kianpour, M., & Kowalski, S. (2019, August 27). An empirical study of security culture in open source software communities. In *2019 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)* (pp. 863-870). doi:10.1145/3341161.3343520

Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security*, *88*, 101640. doi:10.1016/j.cose.2019.101640

Wohlin, C., & Aurum, A. (2015). Towards a decision-making structure for selecting a research design in empirical software engineering. *Empirical Software Engineering*, *20*, 1427-1455. doi:10.1007/s10664-014-9319-7

Wolgemuth, J. R., Erdil-Moody, Z., Opsal, T., Cross, J. E., Kaanta, T., Dickmann, E. M., & Colomer, S. (2015). Participants' experiences of the qualitative interview: Considering the importance of research paradigms. *Qualitative research*, *15*, 351-372. doi:10.1177/1468794114524222

Wood, C. (2019). Ransomware forces New Mexico school district to scrub 30,000 devices. EDSCOOP. Retrieved from https://edscoop.com/ransomware-forces-new-mexico-school-district-scrub-30000-devices/

Xu, S., Meso, P., & Ding, Y. (2016). Information security training customized by risk profile. *Information Security Training Customized by Risk Profile.* Retrieved from https://pdfs.semanticscholar.org/b973/45674743d94be34877d687100f5f3bbd69fe.pdf

Yalof, B., & Chametzky, B. (2016). Mentoring online doctoral students through a community of practice model. *Online Journal of Distance Education and e-Learning*, *4*(2), 39-46. http://www.tojdel.net/journals/tojdel/volumes/tojdel-volume04-i02.pdf#page=46

Yan, Z., Wang, M., Li, Y., & Vasilakos, A. V. (2016). Encrypted data management with deduplication in cloud computing. *IEEE Cloud Computing*, *3*(2), 28-35. doi:10.1109/MCC.2016.29

Yazan, B. (2015). Three approaches to case study methods in education. *Qualitative Report*, *20*, 134-152. Retrieved from https://nsuworks.nova.edu/tqr

Young, D. K., Carpenter, D., & McLeod, A. (2016). Malware avoidance motivations and behaviors: A technology threat avoidance replication. *AIS Transactions on Replication Research*, *2*(8), 1-17.

Young, J. C., Rose, D. C., Mumby, H. S., Benitez-Capistros, F., Derrick, C. J., Finch, T., ... & Parkinson, S. (2018). A methodological guide to using and reporting on interviews in conservation science research. *Methods in Ecology and Evolution*, *9*(1), 10-19. doi:10.1111/2041-210X.12828

Yousuf, T., Mahmoud, R., Aloul, F., & Zualkernan, I. (2015). Internet of Things (IoT) security: Current status, challenges and countermeasures. *International Journal for Information Security Research*, *5*, 608-616. doi:10.20533/ijisr.2042.4639.2015.0070

Zahedi, F. M., Abbasi, A., & Chen, Y. (2017). Fake-website detection tools: Identifying elements that promote individuals’ use and enhance their performance. *Journal of the Association for Information Systems, 16*, 448-484. doi:10.1108/JAIS-01-2016-0045

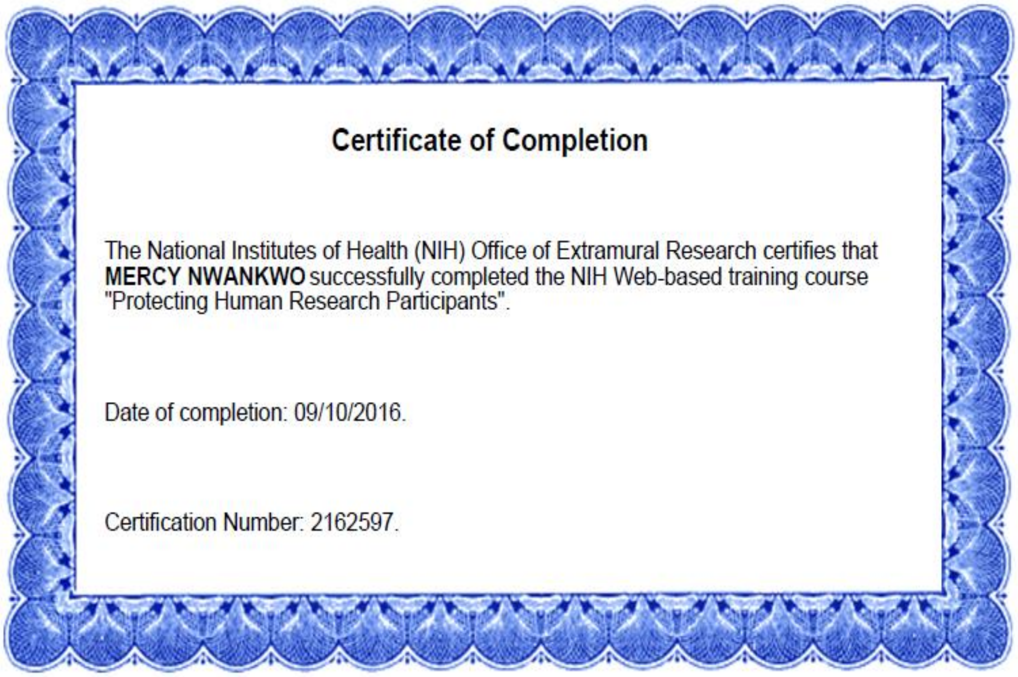
Zamawe, F. C. (2015). The implication of using NVivo software in qualitative data analysis: Evidence-based reflections. *Malawi Medical Journal*, *27*, 13-15. doi:10.4314/mmj.v27i1.4

Zeeck, K. A. (2012). *A phenomenological study of the lived experiences of elementary principals involved in dual-career relationships with children* (Doctoral dissertation, University of St. Thomas). University of St. Thomas Digital Archive. Retrieved from https://ir.stthomas.edu/caps_ed_lead_docdiss/5

Zhang, Z., & Gupta, B. B. (2018). Social media security and trustworthiness: Overview and new direction. *Future Generation Computer Systems*, *86*, 914-925. doi:10.1016/j.future.2016.10.007

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, *60(1),* 1-16. doi:10.1080/08874417.2020.1712269

Appendix A: National Institutes of Health Human Subject Research Certificate of Completion



Certificate of Completion

The National Institutes of Health (NIH) Office of Extramural Research certifies that **MERCY NWANKWO** successfully completed the NIH Web-based training course "Protecting Human Research Participants".

Date of completion: 09/10/2016.

Certification Number: 2162597.

Appendix B: Interview Protocol

INTERVIEW PROTOCOL		
Activity #	What the Researcher will do	What the researcher will say
B1	The researcher will initiate a call at least 10 minutes earlier to communicate with the participant. This is to allow the researcher as well as the participants' time to prepare for the interview session.	Good day sir/ma. This is a kind reminder of the interview session planned for today. It will be due in about 10 minutes time. Thank you for your generosity.
B2	The researcher will set the stage for the interview. This stage set includes introducing the yourself as the researcher to the participants and the introduction of the interview.	Good day Sir/Ma. As a re-introduction, the researcher's name is Mercy Nwankwo. This study attempts to explore the strategies that IT security managers use in the mitigation of data breaches in their school network. The findings from this study may benefit information technology security practice by increasing IT security practitioners' understanding and knowledge of cyber-attacks which may potentially lead to more secured school networks. There is a possibility that successful research in this direction may contribute a positive social change with the potential to provide a more secure and non-threatening online experience to students. The researcher will also like to use this opportunity to inform you that this interview session will be audio recorded for onward transcription later. The audio recording will be for research purposes only and to limit note taking. During this interview, the researcher will also be documenting down important points and may ask questions with respect to provided responses. Please be kindly informed also that you are at liberty to also ask me questions if necessary at any time during this interview session. Thank you.

B3	Ask the participants if they are ready to begin the session	Please, the researcher will want to ask a simple question: Can we start the session now?
B4	If participants' response is in the affirmative, proceed with bringing out your audio recording device, put same on, and get it set for recording	Thank you for your consent. The session starts right away
B5	Start asking one question after the other using the responses from the open-ended questions as the basis for the interview session. Remember to document points when needed, ask follow-up probing questions when necessary, watch out for non-verbal responses or signals, paraphrase where possible and if doing so will help the participant get the question clearer	The researcher will ask you questions one after the order, starting with the first question.
	Interview Questions	
B6	Introduce the overarching research question	What strategies do IT security managers use to mitigate data breaches on their school's network?
B6(1)	Remember to always ask more probing questions, take note of important point raised, rephrase the question, clarify misunderstood response if needed and necessary. Be kind to thank the participant after each question and be cautious of interview time allotted.	Thank you for the response
B6(2)	Ask the first question, next question, …., last question. ↓	Be kind to thank the participant after each question, and be cautious of interview time allotted.
Interview / Survey Questions		

B6(3)	What strategies do IT security managers use to mitigate data breaches on their school’s network? 1. What techniques do you employ to mitigate data breaches? 2. How can you protect and control the flow of data on your network from unauthorized access? 3. How do you manage the challenges faced in implementing these strategies? 4. What is the technical expertise that IT security managers need to be able to improve data breach prevention within an organization? 5. What are some of the setbacks you encountered when responding to data security breaches? 6. What are those skillsets IT security managers lack that are needed to minimize data breaches? 7. How likely will security compliance violation within the organization result in data breaches? 8. How frequently have your organization experienced data breaches? 9. What data breach incidence have you tackled that largely and negatively impacted your organization? 10. What are those factors that can motivate attackers to target an organization’s data? 11. What data security policies and best practices will you suggest that will help mitigate the incidence of data breaches within the organization? 12. How can you reduce the impact or the likelihood of a data breach? 13. What operational IT prevention programs do you have in place that could offer parents and families an increased assurance of their wards’ online safety while in school? 14. What recommendations can you provide that may assist IT security managers and leaders in security in implementing proactive data security measures?
B6(4)	Thank the participant for partaking in the study. Confirm that the participant has an available contact information for follow up questions and concerns. Remind the participant of a member checking taking place in few days to revalidate all his answers provided. End protocol.

Appendix C: Follow-up Member-checking Interview Protocol

Follow-up Member-checking Interview Protocol		
Activity Number	What the Researcher will do	What the researcher will say
C1	The researcher will initiate a call at least 10 minutes earlier to communicate with the participant. This is to allow the researcher as well as the participants' time to prepare for the interview session.	Good day sir/ma. This is to remind you of the member checking session planned for today. It will be due in about 10 minutes time. Thank you for your generosity.
C2	The researcher will set the stage for the member checking session. This stage set should start by thanking the participants for their assistance, input, time, and commitment to the research, especially for the last phone interview session.	Thank you for helping out in the last phone interview session. I highly appreciate your effort, time, input, and contributions towards helping to make this research a success.
C3	The researcher introduces the member checking follow-up interview and set the stage based on the email sent a week ago to the participant containing participants' responses.	Today's session is the member checking stage designed for us to go over the responses you have previously provided. This is to ensure that the researcher accurately captured your responses to the research questions. You are expected to re-validate, confirm or refute the interpretations represented from your responses.
C4	The researcher would now discuss the synthesized interpretations for each question developed from participants' interview responses.	This is the interpretation of the responses provided during our initial phone interview.
C5	The researcher will list each answers provided to each questions by the participant. The participant will listen to each interpretations. I will ask for validations or refute of the interpretations.	Please does the interpretation accurately represent your responses to the interview questions?

C6(1)	If interpretations are not valid, ask for corrections and amendments	Please kindly consent, re-validate or refute, areas or responses whose interpretations were not accurately captured so we can make corrections.
C6(2)	If interpretations are validated, then bring in probing questions that may have emanated from your synthesis which the researcher think may contribute to clarity, increased in-depth information, and improved accurateness of the responses. Probing questions may also be related to other information that may help improve the research knowledge base and contribute to better results of research.	
C7	Conclude the main session by asking the participant(s) for their final input or additions.	Thank you for your help. Please, what do you think you may want to add to this session?
C8	Finally, thank the participants for their time and input. Then collect the distributed sheets from the participant(s)	Thank you so much for your time and input. I highly appreciate.

Appendix D: Letter to Authors for Permission to Use Developed Images

From: huigang liang <huigang.liang@gmail.com>
Sent: Monday, June 3, 2019 7:56 PM
To: Mercy Nwankwo
Cc: xuey@ecu.edu
Subject: Re: PERMISSION REQUEST TO USE DEVELOPED IMAGES

Hi Mercy,

Sure. You are welcome to use it in your dissertation. Is this e-mail enough? Do you need a signed approval?

Best,

Huigang

On Mon, Jun 3, 2019 at 8:28 PM Mercy Nwankwo <mercy.nwankwo@waldenu.edu> wrote:

Mercy Nwankwo
Student ID (A00574945)
Doctor of Information Technology Student
Walden University

Huigang Liang
Department of MIS
College of Business
East Carolina University
Greenville, NC 27858U.S.A.
huigang.liang@gmail.com

Yajiong Xue
Department of MIS
College of Business
East Carolina University
Greenville, NC 27858U.S.A.
xuey@ecu.edu

06-03-2019

PERMISSION REQUEST TO USE DEVELOPED IMAGE (The Process of IT Threat Avoidance)
Dear Liang & Xue,

I hope this e-mail finds you well and in great shape.

I am Mercy Nwankwo, a doctoral student, Information Technology at Walden University. I am working on my thesis of study concerning the IT manager's strategies in mitigating data breaches in their school district network. As being very successful reflecting wordlent research of an IT avoidance mitigation strategy for IT threats, I have selected your study to use as my conceptual framework, and to use your developed image "The Process of IT Threat Avoidance." to improve my work.
Title /Description of your material: Avoidance of information technology threats: a theoretical perspective. MIS quarterly, 71-90.

Authors: Liang & Xue/Avoidance of IT Threats.

Image Title /Page Numbers:
The Process of IT Threat Avoidance as presented by Liang and Xue (2009)
The Research Model as presented by Liang & Xue (2010).

The image permission would include use in my Research work that will be published by the Walden University on school websites in electronic versions for further reference.

I would be grateful if you could provide the caption and credit information in the field below as well as the image files with full permission to proceed with using your developed image in my study.

Thank You
Mercy Nwankwo
Student ID (A00574945)
Doctor of Information Technology Student
Walden University
100 Washington Avenue South
Suite 900
Minneapolis, MN 55401
E-mail: mercy.nwankwo@waldenu.edu
E-mail: mercy.nwankwo@gmail.com
Phone: 832- 518 – 8878

AUTHORS APPROVED / COMMENT:
Name: ____
Written Approval: ____________________________________
Date: ____
Address: ____
Credit line(s)/copyright notice for the material: _____________________
Additional Information: