2020

Exploring Strategies for Enforcing Cybersecurity Policies

Bayo Olushola Omoyiola
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Bayo Olushola Omoyiola

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. Jon McKeeby, Committee Chairperson, Information Technology Faculty
Dr. Donald Carpenter, 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

Exploring Strategies for Enforcing Cybersecurity Policies

by

Bayo Olushola Omoyiola

MS.IT, Walden University, 2017

MBA, University of Sunderland, 2013

B.Tech. Electronic/Electrical Engineering, Ladoke Akintola University of Tech., 2005

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

December 2020

Abstract

Some cybersecurity leaders have not enforced cybersecurity policies in their organizations. The lack of employee cybersecurity policy compliance is a significant threat in organizations because it leads to security risks and breaches. Grounded in the theory of planned behavior, the purpose of this qualitative case study was to explore the strategies cybersecurity leaders utilize to enforce cybersecurity policies. The participants were cybersecurity leaders from 3 large organizations in the southwest and northcentral Nigeria responsible for enforcing cybersecurity policies. The data collection included semi-structured interviews of participating cybersecurity leaders (n = 12) and analysis of cybersecurity policy documents (n = 20). Thematic analysis identified 4 primary themes: security awareness and training, communication, management support, and technology control. A key recommendation is that organizations should have a chief information security officer for oversight of cybersecurity. Employee cybersecurity compliance should be reviewed regularly throughout the year for improvement and desired cybersecurity behavior. The implications for positive social change include the potential for cybersecurity leaders to implement cybersecurity measures that could enhance the public's confidence by assuring them of their data's safety and confidentiality, the integrity of data, and the availability of their services.

Exploring Strategies for Enforcing Cybersecurity Policies

by

Bayo Olushola Omoyiola

MS.IT, Walden University, 2017

MBA, University of Sunderland, 2013

B.Tech. Electronic/Electrical Engineering, Ladoke Akintola University of Tech., 2005

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

December 2020

Dedication

I dedicate this study to my Lord and Savior, Jesus Christ, for giving me the strength, inspiration, motivation, and resources to conduct, write and complete this doctoral study.

Acknowledgments

First of all, I would like to thank my Lord and Savior, Jesus Christ, for making it possible for me to complete this doctoral study. I wish to appreciate my chair, Dr. Jon Mckeeby, for his mentoring, support, motivation, and guidance throughout the period I conducted and wrote my doctoral study. Without his support and motivation, I would still be way behind in this study. I also wish to appreciate Dr. Don Carpenter, my second committee member, and Dr. Jodine Burchell, my university reviewer, for their invaluable feedback.

I would also like to acknowledge the support of my late mother and my late brother for encouraging me and morally supporting me. I would like to appreciate my dad, and my other siblings, for their moral support and motivation. I would also like to thank my wife, and my kids, for their moral support and encouragement. Finally, I would like to thank all my mentors for their tremendous moral support and encouragement throughout this research study.

Table of Contents

List of Tables

Section 1: Foundation of the Study

Background of the Problem

Security has become a significant issue globally; companies over the world are trying to manage security challenges and mitigate security risks. The causes of these security threats are external factors or internal factors (Opderbeck, 2016). Though some of the causes are technical, human factors cause most cases through ignorance or negligence regarding data protection (Manworren, Letwat, & Daily, 2016). Lack of employee cybersecurity policy compliance is a significant threat in organizations (Fritz & Kaefer, 2017). Because employees cause most security incidents, they are the weakest link in cybersecurity (Bauer, Chudzikowski & Bernroider, 2017; Flowerday & Tuyikeze, 2016). But they can become a barrier to threats through adequate security education, training, and awareness programs, which can enhance policy compliance and reduce security incidents (Manworren et al., 2016). Therefore, my objective in this study was to explore the strategies that cybersecurity leaders utilize to enforce cybersecurity policies that prevent security breaches in their organizations.

Problem Statement

The lack of employees' cybersecurity policy compliance has led to a 25% increase in the number of occurrences of cyber-attacks (Kruse, Frederick, Jacobson, & Monticone, 2017). There were 4.5 billion personally identifiable information records stolen in the first half of 2018 because the organizational cybersecurity leaders did not enforce proper cybersecurity measures to prevent data loss (Fielding, 2019). The general information technology (IT) problem is that some organizations encounter security risks

because of their employees' lack of compliance with their cybersecurity policies. The specific IT problem is that some cybersecurity leaders lack strategies to enforce cybersecurity policies in an organization.

Purpose Statement

The purpose of this qualitative multiple case study was to explore strategies used by cybersecurity leaders to enforce cybersecurity policies in an organization. The cybersecurity leaders included information system security officers, cybersecurity managers, and chief information security officers (CISOs). The study population of the study was cybersecurity leaders associated with the enforcement of cybersecurity policies in three large organizations located in southwest and northcentral Nigeria. The implication for positive social change lies in the potential to improve the confidentiality of data, reduction in the occurrence of breaches, enhanced integrity of personal information, continuous availability of services, and the safety of life through improved cybersecurity compliance and awareness.

Nature of the Study

The qualitative methodology is the research method for this doctoral study. Qualitative research explains how, why, and the experience of a phenomenon, thereby giving a more in-depth explanation of motivations, attitudes, and behaviors (Abildgaard, Saksvik, & Nielsen, 2016). Qualitative study is a detailed research methodology, and it helps researchers know and explain the participants' actions (Peck & Mummery, 2017). I used a qualitative method to explore the strategies that cybersecurity leaders utilize for enforcing cybersecurity policies. In contrast, quantitative research involves hypothesis

testing to examine the relationship between the dependent and independent variable(s), statistical analysis of data and generally requires probability sampling techniques for researchers to generalize what all find (Visser, Van Biljon, & Herselman, 2017). This study did not require hypothesis testing, statistical analysis, and probability sampling; therefore, the quantitative methodology was not suitable for this research. Mixed methods involve combining qualitative and quantitative data to provide a fuller solution to problems (Gibson, 2017). My research method did not require quantitative data; therefore, mixed methods research was not appropriate for my research study.

The qualitative design techniques considered for this study were narrative, case study, phenomenological, and ethnography. The case study design is an empirical study that probes a contemporary phenomenon within its real-life context, mainly when the differences between the object of research and meaning is not so apparent (Ebneyamini & Moghadam, 2018). The case study was the most appropriate for investigating my research question, as I investigated in-depth the phenomenon of cybersecurity policy and its implementation. The narrative design validates stories from persons as empirical knowledge sources (Bruce, Beuthin, Shields, Molzahn, & Schick-Mararoff, 2016). The study's purpose was not to gather stories; therefore, a narrative design was not appropriate. The phenomenological research is an in-depth inquiry into people's lived experiences (Bliss, 2016). The study's purpose was not for lived experiences; therefore, the use of a phenomenology design was not appropriate. An ethnographic research approach is a qualitative design utilized to analyze social interactions by investigating shared patterns of beliefs, behaviors, and languages in the same cultural group

(Thornham & Cruz, 2018). The study's purpose was not about any group or culture or ethnicity; therefore, ethnography was not proper for this research study.

Research Question

What strategies do cybersecurity leaders use to enforce cybersecurity security policies in an organization?

Interview Questions

Demographic Questions

1. What is your current job role, and how many years have you spent on the job?
2. How many years of experience do you have in cybersecurity?
3. What other job roles have you held in the field of cybersecurity?

Interview Questions

1. What types of security programs do you manage?
2. What roles within your corporation assist in the development and implementation of security policies?
3. What methods do you utilize to enforce cybersecurity policies?
4. What prompted the need for the enforcement of cybersecurity policies?
5. What methods do you consider the best, and which approach do you consider least effective?
6. What factors influenced your decision to use the type of approach you use to implement cybersecurity policies?

7. What do you consider the merits of enforcing cybersecurity policies? What has been the impact on employee compliance?
8. What challenges do you face during cybersecurity policy implementation?
9. What internal threats and human factors affect enterprise information security and employee cybersecurity policy compliance in organizations?
10. What are the external threats that affect organizational information security?
11. In what ways and how often do you review the security architecture of your organization?
12. In what ways and how often do you review employee cybersecurity policy compliance?
13. What solutions do you use to overcome compliance challenges?
14. What solutions have you put in place to mitigate security threats?
15. What type of training programs does your firm organize for staff members to educate them on security, data privacy, and compliance?
16. What impact has the education had on the risk culture of your organization?
17. How do you stay abreast of emerging technologies and keep yourself updated in the continually evolving cybersecurity field to manage the security of your company's information assets, data, and resources?

Conceptual Framework

The conceptual framework for this qualitative study is the theory of planned behavior (TPB) created by Icek Ajzen in 1985 (Ajzen, 1985). The TPB postulates three determinants of intention: attitude to behavior, subjective norms, and perceived

behavioral control (Sommestad, Karlzen, & Hallberg, 2019). The intention to perform a behavior and perceived control of behavior is predictable by behavioral performance. In general, a stronger intention to perform a behavior emerges as attitude becomes more positive, and subjective norms and perceived behavioral control becomes greater. Attitude toward behavior is the extent to which behavior gets classified as favorable or unfavorable. The subjective norm is the perceived social pressures to do the behavior. Perceived behavioral control implies the extent of ease or difficulty involved in behavior from people's viewpoints (Ajzen, 1991). Behavioral intention is an essential tenet of the TPB (Ifinedo, 2016), and it implies the readiness to do a given behavior (D'Arcy & Lowry, 2017). The TPB considers behavior as the outcome of intentions and behavioral control, with intentions determined by some beliefs, which comprise norms, attitudes, and perceived behavioral control (Sommestad et al., 2019).

The TPB has been a useful framework for research on cybersecurity policy implementation and information security compliance behavior. Ifinedo (2016) found the TPB suitable to explain all behavioral actions and used it in his research on behavioral intention. Sommestad et al. (2019) also used TPB as a framework for a study on information system security behavior and addressed the sufficiency assumption in the context of security policy compliance behavior.

Understanding the strategies for enforcing cybersecurity policies is essential to reduce risks and enhance employee compliance and the risk culture. The TPB is appropriate for this research because TPB focuses on attitude towards behavior, information security awareness, and intentions to comply with policies as determinants of

employee cybersecurity policy compliance. The application of the strategies can improve risk culture and improve employee cybersecurity policy compliance in an organization. The basis of implementing cybersecurity policies in an organization is to ensure cybersecurity compliance and safety. Implementing cybersecurity policies in institutions may bring about better data protection and cybersecurity compliance. Employees and customers may benefit from security strategies because their application may ensure their data and resources' safety. The TPB facilitated a better understanding of the strategies for cybersecurity policy implementation.

Definition of Terms

Breach: A breach refers to an unauthorized compromise, disclosure, or access to personal information (Hemphill & Longstreet, 2016).

Compliance intention: Compliance intention born out of organizational security efforts refers to paid workers' intention to secure their company's information assets against security breaches (Hwang, Kim, Kim, & Kim, 2017).

Cybercrimes: Cybercrimes refer to criminal activities done through information systems and communication networks against targeted networks to steal confidential data or hacking networks (Bergmann, Dreißigacker, Von Skarczinski, & Wollinger, 2018).

Cyber-attack: Cyber-attack refers to the intentional exploitation of computers and networks utilizing malicious methods and devices (Samtani, Chinn, Chen, & Nunamaker, 2017).

Information security: Information security refers to the process of protecting any stored information, data, or information systems, from unauthorized use, disclosure, disruption, tampering, or fraudulent use (Bernik & Prislan, 2016).

Information security policy. An information security policy refers to formal directives that highlight the management's rules on information security, access, and information sets and consequences for not adhering to the rules (Karlsson, Hedstrom, & Goldkuhl, 2017; Niemimaa & Niemimaa, 2017; Yazdanmehr & Wang, 2016).

Insider threats: Insider threats occur when employees who have authorized access to their organization's information system abuse their rights and attack the system (Tyler, 2016).

Security education, training, and awareness: Security education training and awareness refers to formal programs and efforts organized by organizations to educate, train, and enhance the security awareness of their employees and end-users on security threats, security measures, and their security responsibility in protecting their passwords, data, and information system against unauthorized access and other security threats (Hwang et al., 2017)

Security strategies: Security strategies refer to defense actions used to guard against unauthorized access to an information system (Tan & Yu, 2018).

Assumptions, Limitations, and Delimitations

Assumptions

Assumptions define the researcher's preconceptions, beliefs, and subjective perceptions that are considered true (Rahi, 2017; Twining, Heller, Nussbaum, & Tsai,

2017). For the multiple case study, I assumed that the participants' findings from each organization reflect the firms' actual state. I also assumed that all the participants answered each interview question accurately. I also assumed that all the participants had all the necessary experience and give me the required knowledge of how they enforce cybersecurity policies.

Limitations

Limitations define the shortcomings, weaknesses, or restrictions that limit the degree of realization in a study (Brusse, Kach, & Wagner, 2016). A potential limitation of this research was the sample size. However, the sample size was not an issue because organizational documents supported the participants' responses, ensuring data saturation. A second potential limitation was that the cybersecurity leaders did not have much time for an interview due to their busy schedules, but this was not an issue because they created time for the interview.

Delimitations

Delimitations define the boundary limits that a researcher sets for the research (Brusse et al., 2016; Snelson, 2016). The delimitations of this study are the criteria set for the research. The first delimitation was the location, which was southwest and northcentral Nigeria. A second delimitation is that the study was limited to three firms and large organizations with four cybersecurity policy enforcers. A third delimitation is the study's limit to participants who are cybersecurity leaders involved in enforcing cybersecurity policies.

Significance of the Study

Contribution to Information Technology Practice

Globally, the number of cyber-attacks against organizations has increased dramatically. Several security breaches have occurred due to social links and insider influence (Opderbeck, 2016). Many of these cybersecurity attacks occurred due to the nonexistence of a matured risk culture in the targeted organizations, hence the need to enforce cybersecurity policies that will help reduce the security risks and assist in preventing security breaches and improve cybersecurity compliance. This research study may contribute to the cybersecurity body of knowledge because it includes strategies for implementing cybersecurity policies. This research's findings may assist cybersecurity managers by providing them with strategies for implementing cybersecurity policies, overcoming the challenges that come with the process, understanding cybersecurity compliance better, and developing, enforcing, and implementing better cybersecurity policies. This study's findings may offer a holistic approach to the implementation of cybersecurity policies. The study's findings may also help improve the cybersecurity culture of various organizations that require the recommended cybersecurity measures.

Implications for Social Change

The implications for positive social change of this research lies in the potential for the strategies in the study's results to impact the public significantly. Security breaches usually have a high effect on society because of the socioeconomic impact caused by the loss of data and financial losses. The strategies for preventing the loss of confidential data from this study's findings may reduce the occurrence of breaches. The strategies can also

enhance the public's confidence because the security measures may assure them of their data and resources' safety, confidentiality, and privacy. The integrity of the confidential information of the public may also get enhanced through security awareness. The strategies of this study may also benefit various sectors of the economy. After implementing appropriate security education, training, and awareness and activating cybersecurity policies, there may be continuous availability of services and life safety.

Review of the Professional and Academic Literature

Overview

The literature review provides a background to cybersecurity policy implementation and employee cybersecurity policy compliance. Excellent literature reviews comprise constructive and critical analysis and synthesis of current literature, knowledge, and discussions on the theory and concepts and contain recommendations for future studies (Torraco, 2016). This literature review section includes a review of published works on cybersecurity topics related to this study, application to the applied IT problem and a review of published works on this doctoral study's conceptual framework and rival theories. The cybersecurity topics include cybersecurity policies, employee cybersecurity policy compliance, and the root cause of security attacks and breaches. The application to applied IT problems focuses on the strategies for implementing cybersecurity policies. The literature review also includes the conceptual framework (TPB) and rival theories such as institutional theory, protection motivation theory (PMT), deterrence theory, technology acceptance model (TAM), the theory of

reasoned action (TRA), rational choice theory (RCT), and social cognitive theory (SCT) and their application to case studies.

This literature review contains a review of articles from the Thoreau Multi Database, and EBSCOHost Academic Search in the Walden University's Library, Elsevier, ScienceDirect, Emerald Insight, Google Scholar, Taylor & Francis, and ACM Digital Library, etc. The references were verified using Ulrich's periodicals directory to ensure that the references were peer-reviewed. The total sum of references for the literature review only was 203 articles. Out of which, 187 (92.1%) articles are from peer-reviewed journals and out of which 173 articles (85.2%) are within 5 years of the anticipated graduation date (see Table 1 for more details).

Table 1

Distribution of References

	Literature review		Section 2		Proposal	
Reference status	Count	Percentage	Count	Percentage	Count	Percentage
Peer-reviewed	187	92.1%	97	91.51%	294	92.2%
Non-peer-reviewed	10	4.9%	5	4.72%	15	4.7%
Books	5	2.5%	3	2.83%	8	2.5%
Web pages	0	0%	1	0.94%	1	0.3%
Other	1	0.5%	0	0%	1	0.3%
Total	203	100%	106	100%	319	100%
Reference age						
Less than 5 years old	173	85.2%	101	96%	284	89%
Five years old and more	30	14.8%	4	4%	35	11%
Total	203	100%	106	100%	319	100%

Cybersecurity

Cybersecurity policies. Cybersecurity policies encompass an organization's management's expectations concerning users' behavior patterns of a specific system. The security policy serves as a layout of a framework of expectations for the organization's

security program, including specifications for system controls (Almeida, Carvalho, & Cruz, 2018; Helil & Rahman, 2017). Cybersecurity policies are principles of an organization's actions for its end users that serve as an essential mechanism toward implementing cybersecurity to protect its IT assets and resources (Soomro, Shah, & Ahmed, 2016). An organization's cybersecurity policy will typically comprise regulations for an organization's employees to follow regarding using and accessing the organization's information systems (Yazdanmehr & Wang, 2016).

Organizations communicate their cybersecurity expectations and the consequences of not complying with their objectives through their cybersecurity policy (Niemimaa & Niemimaa, 2017). Cybersecurity policies tackle acceptable technology usage, social media, and sensitive information (Han, Kim, & Kim, 2017). A cybersecurity policy must be adequately clear, well outlined, and provide regulatory guides for action for clear guidance (Karlsson et al., 2017), because ambiguity in cybersecurity policies can reduce employee policy compliance.

Organizations must aspire and develop mechanisms to manage employees who have access to clients' information (Chua, Wong, Low, & Chang, 2018). Cybersecurity policies are most important for the security architecture of any organization. Securing any organization's information assets entails technical controls and nontechnical controls such as managerial or administrative mechanisms. Enhancing the nontechnical measures also enhances the company's security posture (Shepherd & Mejias, 2016). Furthermore, technical controls like firewalls, antivirus programs, likewise intrusion detection systems, every organization are dependent on cybersecurity policies to tackle non-technical

activities of cybersecurity (Cram, Proudfoot, & D'Arcy, 2017). A holistic view of organizational cybersecurity must involve people, processes, and technology to reduce security risks (Evans, Maglaras, He, & Janicke, 2016; Ritzman & Kahle-Piasecki, 2016).

Ensuring that the organization's staff or workforce comprehends cybersecurity policy can reduce cybersecurity risks (Mamonov & Benbunan-Fich, 2018). The new-hire orientation programs offer an opportunity to train individual employees on an organization's cybersecurity policy (Bauer, Bernroider, & Chudzikowski, 2017). The onboarding process involves the following: employees are mandated by law to sign, indicating acknowledgment and acceptance of the cybersecurity policy (Bauer et al., 2017). This specific reduction in risk may be due to users' knowledge about acceptable systems usage and existing security measures while they read the security policy. Additionally, security education training and awareness programs can enhance employee cybersecurity policy compliance and improve implementing cybersecurity policies (Cong, Dang, Brennan, & Richardson, 2017; Flowerday & Tuyikeze, 2016). Employee cybersecurity policy compliance makes work more comfortable and reduces privacy breaches in organizations (Balozian & Leidner, 2017; Lee, Lee, & Kim, 2016a). Constant awareness of the cybersecurity policy and its terms also lead to policy compliance (Yazdanmehr & Wang, 2016).

In the absence of compliance, the most elaborate cybersecurity policy will be ineffective, being countermeasures to security issues (Yazdanmehr & Wang, 2016). Some employees are not usually compliant with organizational cybersecurity policies (Belanger, Collignon, Enget, & Negangard, 2017). Noncompliant behavior patterns like

postponement or intentional resistance to security policies can harm the organizations (Belanger et al., 2017). Inadequate compliance by an employee may lead to adverse cybersecurity outcomes, but compliance with cybersecurity policies is a significant factor in organizational effectiveness (Almeida et al., 2018). Compliance is a must for companies' regulatory compliance in their industry (Chen, Chen, & Wu, 2018a).

Cybersecurity policies at various levels. Organizational security policies satisfy cybersecurity requirements at the enterprise, user, and system levels (Cram et al., 2017). Cybersecurity policies provide security expectations at many levels. At the organizational or corporate level, security policies mainly provide directives for guiding overall cybersecurity, including regulation for handling and sharing sensitive data (Cram et al., 2017). Organizational leaders maintain the use of an executive-level security policy pattern designed to articulate the security vision, either overarching strategic direction for all security efforts (Cram et al., 2017). Organizations also provide a kind of a user-level security policy that focuses on cybersecurity issues at a more granular level. User-level policies are mainly concerned with delivering expectations for acceptable use of systems, involving characteristics such as policies based on a passcode, policies based on e-mail, and policies based on internet usage (Belanger et al., 2017).

User-level policies give specific directives for end-users, whereas executive level or corporate level policies guide cybersecurity leaders. Security policies for security program levels usually state prescribed components of security programs and assign responsibilities to implement security program elements, program management, and incident management. Security program policies can highlight the steps for prolonging

business continuity with robust cybersecurity incident management (Steinbart, Raschke, Gal, & Dilla, 2016). Control level policies entail data and information system classification in terms of data sensitivity levels, including the criticality of information system components.

System and control policies can establish controls usually for handling, labeling, transportation, and destroying various sensitive data (Helil & Rahman, 2017). The remaining aspects of information system security that system and control policies will address are data recovery procedures and incident management procedures. System and control policies are mainly directed to target specific system components or hardware, like data servers, network components, or applications. Such policies relate to the system and control level involving the network access policy, web server security policy, acceptable encryption policy, application service provider policy, extranet policy, and the authentication passcodes policy (Auxilia & Raja, 2016). Cybersecurity programs can also provide standards, guidelines, baselines, and procedures to shape various organizations staffs' cybersecurity behavior patterns.

Standards. Cybersecurity standards are an essential phenomenon of an organization's cybersecurity program. Cybersecurity standards provide details to cybersecurity policies like details on methods, techniques, or devices (Niemimaa & Niemimaa, 2017). The senior management level is responsible for issuing mandatory cybersecurity standards (Chul Ho, Xianjun, & Raghunathan, 2016). Standards are collections of best practices established by different regulatory bodies in specific industries (Niemimaa & Niemimaa, 2017). Organizations mainly use such industry-wide

security standards to maintain security controls (Chul Ho et al., 2016; Niemimaa & Niemimaa, 2017). However, cybersecurity standards give extra information to security policies and must be established internally or done by industry-wide various regulatory bodies.

Guidelines. Cybersecurity guidelines are often similar to cybersecurity standards because they provide extra elaborations on security policies. But unlike cybersecurity standards, security guidelines are not compulsory (Flowerday & Tuyikeze, 2016). Security guidelines provide best practice methods or techniques.

Baselines. Baselines involvement is mandatory, and it reduces security risk within applications. Cybersecurity baselines (or benchmarks) give room for additional information on security requirements in cybersecurity policies inference to devices or applications whereby specific settings or parameters are mostly required (Niemimaa & Niemimaa, 2017). The initial establishment of baselines or benchmarks can help an organization identify and adopt cybersecurity best practices (Niemimaa & Niemimaa, 2017). Security baselines enhance security settings or parameters, usually based on known vulnerabilities.

Procedures. Cybersecurity procedures aid in providing a uniform format of implementing policies in regions where many individuals in various roles are part of the process. Cybersecurity procedures give detailed instructions, such as step-by-step, to implement security controls in line with cybersecurity policies, standards, or guidelines (Hanus & Wu, 2016). Procedures state the order in which all the employees should address given tasks and the roles and responsibilities of all entities involved in the

process. Similarly, formal procedures ensure balance in cybersecurity (Flowerday & Tuyikeze, 2016) and the smooth operations of cybersecurity.

Security policy management. The emergence of IT policies like cybersecurity policies and privacy policies should aid organizations in meeting their objectives. Cybersecurity policies are mainly a subset of a broader IT governance strategy. IT governance's two primary purposes are the alignment between IT activities and organizational goals and the generation of value from IT (Wilkin, Couchman, Sohal, & Zutshi, 2016). IT governance also involves providing procedures for enacting policies related to employees' actions while interacting with organizational information systems (Alreemy, Chang, Walters, & Wills, 2016). In this direction, IT governance is most important in controlling the IT decision-making process and proposing to increase benefits from IT investment infrastructures in place (Alreemy et al., 2016). Organizations use diverse strategies to achieve their specific target in terms of IT goals. Cost and strategy are two factors that organizations utilize regarding cybersecurity policy management annually (Clemons, Dewan, Kauffman, & Weber, 2017; Such, Gouglidis, Knowles, Misra, & Rashid, 2016).

Organizations in the healthcare sector and financial sector may be required by law to meet regulatory requirements in broad areas like information privacy and cybersecurity (Wilkin et al., 2016). IT policies serve as a catalyst in which organizations meet such needs. Organizations must comply with legal, regulatory, or compliance requirements, establish efficient and proactive security management practices and policies, and enforce compliance with such requirements (Laube & Bohme, 2016).

Policy monitoring and enforcement. Monitoring and enforcement of policies are critical components of cybersecurity governance. Policy monitoring means controlling and evaluating the policy's lifecycle, managing it, and updating it when necessary (Estevez, Janowski, & Lopes, 2016). Cybersecurity policy monitoring can be performed by IT personnel or by internal auditors delegated by organizational management. Policy monitoring may involve the use of reports that show how policy objectives and impact are received, policy implementation processes, and progress reports on policy outputs and outcomes (Estevez et al., 2016). Policy evaluators may solely rely on feedback gotten from policymakers and end-users.

The enforcement of cybersecurity policies is also vital in securing organizational information systems (Choi, 2016). Organizations, including government organizations, enforce security policies to achieve the intended security and privacy levels (Pussewalage & Oleshchuk, 2016). Security managers can act as enforcers of cybersecurity policies through surveillance and monitoring employee activities to determine violations or deter potential violators (Choi, 2016). Moreover, security managers can be timely in using cybersecurity software to avoid breaking policies (Choi, 2016). For example, institutions can implement a cybersecurity policy regarding passcodes by mandating that passcodes should be of a particular length and strength (Florencio, Herley, & Van Oorschot, 2016; Guo & Zhang, 2017). Policy enforcement involves sanctioning employees who have violated policy and providing education to offenders (Choi, 2016).

Policy review. Cybersecurity leaders should regularly review cybersecurity policies to ensure that they remain relevant and proffer practical security solutions. As

technology continues to evolve, new threats and vulnerabilities emerge, the policies need to abreast of the situation (Choi, 2016). Security policy reviews foster the policies' effectiveness and determine whether the policies need to be updated to reflect organizational changes (Almeida et al., 2018). During a policy review, cybersecurity managers get feedback on the security policy from stakeholders, after which they analyze the findings in other to conclude to determine policy effectiveness, policy relevance, and monitor policy compliance (Estevez et al., 2016). The review process entails examining all security incident data and identifying areas of the security policy that need to be modified (Estevez et al., 2016). Policy review is beneficial to establish the relevance of cybersecurity policies and identify any policy shortcomings.

Root-causes of security attacks and breaches. Security attacks and breaches exist because of factors such as external attackers, internal threats, service providers, and theft (Opderbeck, 2016). Human elements and technical causes are usually the root cause of these attacks (Opderbeck, 2016). The human causes could be deliberate or non-deliberate, whereas the technical root cause could be system or process failures (Fritz & Kaefer, 2017). The effects of these data breaches are usually much because they cause loss of organizational finance, reputation, data, and resources (Ghorbel, Ghorbel, & Jmaiel, 2017). The breaches are attacks on the confidentiality, integrity, or availability of data in an information system (Zafar, Ko, & Osei-Bryson, 2016). Hence, breaches impact consumers' confidence and trust directly affected by these attacks (Carre, Curtis, & Jones, 2018). Breaches are causable by unauthorized access to classified information such as personally identifiable information, personal health information, or private

financial information. The accompanying subsections review the four leading causes of breaches.

External causes. External causes are one of the three primary sources of breaches affecting the information system of organizations. Companies encounter external security threats such as hackers, unauthorized access, malware, viruses, and theft of data and information assets (Cooper, 2016). Six years ago, Target experienced a data breach worth five hundred million dollars due to an external vendor (Hemphill & Longstreet, 2016).

Firms also come across external threats such as industrial espionage, hackers, social engineering, partners, environmental disasters, and revenge attacks from a disgruntled former employee or other attackers. Usually, the attackers look for vulnerabilities in the organization network and information systems and exploit them. External threats come from different sources, and their targets and approaches differ (Cooper, 2016). While some target the weakness of the human side of cybersecurity, some exploit the technical vulnerabilities of the information system.

Hackers and security breaches. There will always be hackers who search for modern techniques to harm people (Tarlow, 2019). A recent study explained that hackers caused 43% of the mega breaches in organizations (Fritz & Kaefer, 2017). Jeong, Lee, and Lim (2019) decried the effect of breaches on some firms' economic performance and market value. When exploiting organizational information systems' technical vulnerabilities, hackers usually look for ways to bypass technical controls such as encryption, intrusion detection system, firewall, etc. (Fritz & Kaefer, 2017). Another

approach hackers use to carry out data and privacy breaches is to lure end-users to visit their malicious websites to have unauthorized access to their confidential information. Besides, hackers use network sniffing and exploitation of weak passcodes (Fritz & Kaefer, 2017; Ranjan & Om, 2016). These are part of their gimmicks.

Similarly, external attackers use social engineering to compromise the security of organizational information systems. Through social engineering, external hackers target users within a company through manipulation, deception, and persuasion to influence the end-users to do things that will weaken their network and information system's security. Mouton, Leenen, and Venter (2016) decried that social engineering's continuous training victims have become a challenging task because of the high rate. The social engineering tools hackers use to deceive users include phishing e-mails and malicious websites (Jensen, Dinger, Wright, & Thatcher, 2017; Perrault, 2018).

The hackers' techniques include exploiting end-users' behavior and adding dangerous attachments or website links in the users' e-mails. Similarly, hackers use messages that appeal to emotions to deceive a particular target group. The phishing e-mails with content tend to be more persuasive in convincing end-users to click on risky website links. Sometimes, the target groups of the external hackers are employees of a particular organization. The hackers lure them into providing confidential information that is capable of compromising the network of the organization. The phishing attack, which involves targeting an individual or a company, is called Spear Phishing. In contrast, the one that focuses on a high-level employee of an organization is called Whaling (Goel & Jain, 2017).

External cybercriminals also use malware, worms, trojan horses, and viruses to infect networks of organizations. The hackers also use website re-directs, website defacements, or denial of service to attack organizations (Jensen et al., 2017). Another external threat is ransomware. Ransomware is used by hackers to disclose and attack the modern-day IT information system by taking advantage of its vulnerabilities (Kruse et al., 2017).

Another external threat to the information systems of companies is Industrial espionage. Industrial espionage is a technique used to gather and steal confidential information, such as trade secrets (Soilen, 2016). Industrial espionage usually involves an organization spying on another organization, though individuals can also carry it out. Industrial espionage requires that systems on the network are not as risky and expensive as traditional methods (Soilen, 2016). Therefore malicious agents use industrial espionage to get a competitive edge over their rivals. Sometimes, an insider is used by a malicious agent to collect data for the other organization (Heickero, 2016). Heickero (2016) and Wirtz and Weyerer (2017) explained that disgruntled employees also indulge in the act of industrial espionage to disclose organizational information with rival competing companies

Insider threats. Individuals within an organization can significantly affect the level of security of organizational information systems. Insider threats remain the most significant security threat to organizations' information systems, though some companies neglect to focus on them (Bartnes, Moe, & Heegaard, 2016). Luna, Rhine, Myhra, Sullivan, and Kruse (2016) decried cyber threats and security risks in the healthcare

industry and listed insider threats as one of them. The threat posed by insiders, such as employees, is significant even in organizations that have complex cybersecurity programs (Fritz & Kaefer, 2017; Sawyer & Hancock, 2018). Consequently, it may be beneficial for organizations to focus more on cybersecurity resources towards mitigating threats from within the organization. Insider threats can be intentional or unintentional (Hills & Anjali, 2017; Opderbeck, 2016) and may have different causes (Gheyas & Abdallah, 2016; Hills & Anjali, 2017). A comprehensive cybersecurity program should consider both unintentional and intentional insider threats.

Employee actions might result in a breach of cybersecurity, even if they did not intend to cause such a violation. Unintentional, employees' risky behavior is often due to a lack of security awareness (Ogutcu, Testik, & Chouseinoglou, 2016). Klein and Luciano (2016), in their study on Brazilian information security users, decried a lack of security and privacy concerns among employees. Some of them unintentionally fall victim to phishing e-mails. Manworren et al. (2016) explained that ignorance of the employee or his negligence on data protection and noncompliance with company policy or guidelines is usually the root cause of most security breaches. Other unintentional insider actions could be visiting websites that are not work-related, selecting insecure passcodes, writing down passcodes on sticky notes, or clicking on phishing links on web sites (Niblett, 2016). Internal information system users may also engage in omissive security behavior.

Insider threats may also be intentional. The behavior of insiders may range from non-malicious to malicious acts (Niblett, 2016). Thus, an employee's actions may be

unintentional and due to carelessness or ignorance, intentional but non-malicious, or intentional and malicious. Computer abuse, information system misuse, violation of policy, and cybersecurity policy abuse are examples of deliberate insider threats (Omar, Mohammed, & Nguyen, 2017). Employees may engage in computer abuse in the form of hardware or software theft, data modification, or computing service disruption. Employees can also participate in system misuse. Information system misuse may include using company computers for non-work-related activities or unauthorized access to confidential information (Homoliak, Toffalini, Guarnizo, Elovici, & Ochoa, 2019). Intentional behavior also includes information theft, sabotage, or espionage (Hills & Anjali, 2017). Employees may also perform more direct, malicious, and intentional violations of cybersecurity policies that may harm information systems. For example, employees may transfer sensitive data to their mobile devices, modify security configurations, or share confidential information with third parties outside the organization (Das & Khan, 2016; Homoliak et al., 2019). Malicious activity by insiders is associated with scams, fraud, and social engineering incidents (Niblett, 2016). Such intentional, malicious actions by employees can have adverse effects on the availability, integrity, and confidentiality of data in a company's network. Deliberate violation of employees' security policies may be more common when employees have a negative attitude towards security controls or when employees are non-cooperative with security policies (Hwang et al., 2017). Insiders with malicious intent pose a significant threat to information systems, mainly because they often have easy access to such systems.

Intentional actions by insiders may not always be with malicious intent. Employees may put information systems at risk due to carelessness or ignorance. For example, employees may leave an unattended computer in a logged-in status out of negligence. Also, insiders who are being mischievous or insiders who have an attitude of resistance towards cybersecurity policies may cause security incidents (Homoliak et al., 2019). Non-malicious, employees' risky actions may be due to a lack of knowledge or awareness of such actions' consequences. Such activities may include clicking insecure links or opening attachments in e-mails, passcode sharing, or writing down passcodes (Homoliak et al., 2019). Although insiders may lack malicious intent, their interactions with information systems directly or indirectly lead to security breaches.

Insiders often have elevated privileges and know an organization's information system, making it easy to bypass security measures and harm the system (Burns, Posey, Roberts, & Lowry, 2017). Safa, Maple, Watson, and Von Solms (2018) explained that motivations and opportunities are primary factors for understanding insider threats. Detecting and preventing insider threats may be more challenging than other threats because perimeter countermeasures like firewalls and intrusion detection systems are ineffective against insider threats (Homoliak et al., 2019). Furthermore, risky insider behavior may affect a company's cybersecurity indirectly by creating security vulnerabilities that can be exploited by malicious outsiders (Hills & Anjali, 2017). These risks make insider threats something organizations need to worry about and tackle.

Business partners. Many organizations rely on business partners for functions and services. For example, healthcare providers may depend on business partners to

perform data analyses, quality assurance, or benefits management in the healthcare sector. Such partnerships may provide cybercriminals an avenue to access organizational information, as business partners and providers often have some access to the organization's network. Mehraeen, Ghazisaeedi, Farzi, and Mirshekari (2016) decried the security risks in healthcare cloud computing and service providers' data handling. Sensitive organizational sensitive data can also be exposed during business transactions such as mergers, consulting, auditing, or joint ventures. Vulnerabilities created through such business transactions can be exploited by the business partners or by third-party malicious attackers. Hills and Anjali (2017) explained that business partners' threats might be challenging to mitigate, as these external entities often require elevated privileges in an organizational network to perform their functions or offer their services.

Lost or stolen devices. Removable or portable electronic devices are another significant source of data breaches. Data breaches in health institutions occurred as breaches that resulted from the usage of laptops, portable electronic devices, and paper records (Homoliak et al., 2019). Fritz and Kaefer (2017) did a study covering ten years and explained that 29% of mega violations within those ten years involved stolen or lost portable electronic items. These studies indicate that the loss or theft of information system devices poses a significant threat to organizations' information system security. The loss of portable electronic devices such as laptops, tablets, storage disks, tapes, or CDs is often associated with carelessness by employees entrusted with such company devices (Homoliak et al., 2019). In this respect, the threat posed by lost devices may be considered an insider threat. Portable devices containing sensitive data can also be stolen

by employees or outsiders, who may exploit the data for personal purposes or sell the information for gain (Homoliak et al., 2019). Theft of portable devices can also occur as part of an industrial espionage scheme (Homoliak et al., 2019). Also, mobile devices may get lost during interactions with trusted business partners or during repairs (Homoliak et al., 2019). In essence, lost or stolen devices can negatively affect information system security, and this threat is often associated with careless employees, business partners, or industrial espionage.

Employee policy compliance. The Organizations institute cybersecurity policies as a means of safeguarding their information systems and technology assets based. The effectiveness of these kinds of policies is affected by the compliance behavior of members of the organization (Elifoglu, Abel, & Tasseven, 2018). This study reviews the factors influencing employees' compliance with policies and regulations, consisting of intrinsic and extrinsic factors.

Intrinsic determinants of compliance. Intrinsic determinants are the kind of determinants affecting behavior from within the individual (Safa et al., 2015). The essential elements may be self-sustaining and may include internal motivations like attitudes towards the policy or regulation, ethical beliefs, or perceptions about the ability to comply with the policy or regulation (Hwang et al., 2017). These kinds of determinants can affect a user's compliance behavior pattern either positively or negatively. For instance, users are more likely to engage in a behavior pattern if they expect some intrinsic benefit from the behavior pattern (Doherty & Tajuddin, 2018; Niblett, 2016). Employee compliance behavior patterns may also be affected by other intrinsic determinants like cybersecurity awareness, self-efficacy, and employee stress.

Attitude towards cybersecurity policy. An employee's attitude towards a specific behavior pattern simply refers to the orientation of the individual's feelings towards engaging in the behavior pattern, and the emotions can be positive or negative (Safa et al., 2015). Da Veiga (2016) explained that the employees' knowledge of security policies positively impacts the organization's security culture. He also explained that the organization's security culture affects the implementation of the information security policy. In other words, cybersecurity policy compliance influences cybersecurity culture and vice versa (Da Veiga, 2016).

Formation or development of an attitude involves evaluating an idea, event, activity, and attitude that can range from very positive to very adverse outcomes (Safa et al., 2015). While, the results of a study by Menard, Bott, and Crossler (2017) indicated that Cybersecurity managers with appealing security measures got a higher intention to comply with security requirements stipulated. Menard et al. (2017) opined that employees might have a more positive attitude towards compliance when they are involved in securing information systems. Kim and Han (2019) identified and noted threat appraisal and response cost as predictors of attitude towards security policy compliance. Park, Kim, and Park (2017a) also opined attitude towards misuse of cybersecurity policies as a factor affecting Cybersecurity policy compliance, with the perceived severity of sanctions being a predictor of attitude displayed. In summation, these studies give evidence that user attitudes towards cybersecurity policies can affect their compliance behavior.

Kim, Kim, and French (2015) investigated behavioral factors affecting employee cybersecurity policy compliance. They utilized a cybersecurity framework and found that attitude towards compliance, beliefs, and self-efficacy affect compliance. Kim et al. (2015) opined that users will consider the cost and benefits of compliance when deciding whether to comply with or violate the policy. The attitude towards compliance will be more favorable when the benefit of compliance outweighs the cost of compliance or the benefit of noncompliance (Kim et al., 2015). Safa et al. (2015) revealed that factors like commitment, involvement, and employees' attitudes towards compliance with Cybersecurity policies could influence policy compliance. The cybersecurity involvement has to do with aspects like sharing cybersecurity knowledge, collaboration, cybersecurity experience, and intervention (Safa et al., 2015).

Cybersecurity knowledge sharing can also be used as an approach to increase cybersecurity awareness. Cybersecurity collaboration helps users to gain adequate knowledge about security breaches while reducing the cost of knowledge acquisition. Cybersecurity experience helps them mitigate inherent cybersecurity risks. Cybersecurity knowledge and experience affect cybersecurity behavior patterns (Safa et al., 2015). The employees' commitment to organizations could be due to aspirations for promotion, personal achievement, or reputation, in the order of their needs. When employees are committed to their organization, they are less likely to take the risk of breaking the rules and violating cybersecurity policies as this could jeopardize their career aspirations, which understandable (Safa et al., 2015).

Similarly, Belanger et al. (2017) revealed that the attitude towards compliance with Cybersecurity policies is dependent on the perceived severity of the security threat and vulnerability (Belanger et al., 2017). The more vulnerable users felt, the more likely they were to comply with a policy (Belanger et al., 2017). These researchers all identified or noted attitude towards compliance as a factor affecting compliance with security policies. However, contrary to the studies mentioned above, Herath and Rao (2009) revealed that employees' attitudes towards security policies do not affect their intention to comply with organizations' policies with high organizational commitment and monitoring. Instead, self-efficacy, social influence, and perception of threat severity impact employees' policy compliance intention (Herath & Rao, 2009).

Self-efficacy. Self-efficacy is a personal perception of confidence in one's ability to comply with cybersecurity policies (Johnston, Warkentin, Mcbride, & Carter, 2016). A review of self-efficacy resources related to cybersecurity shows the pros and cons of the effects of self-efficacy on employees' intentions to comply with cybersecurity policies. Some researchers found a positive influence of self-efficacy on the intention to comply with cybersecurity policies or rules (Johnston et al., 2016; Mwagwabi, McGill, & Dixon, 2014). A study conducted explored user compliance with passcode policies, Mwagwabi et al. (2014) found and discovered that passcode self-efficacy strongly influenced users' passcode policy compliance intentions. Users' confidence in their ability to create strong passcodes correlates with their likelihood to comply with passcode guidelines (Mwagwabi et al., 2014). Bulgurcu, Cavusoglu, and Benbasat (2010) opined that self-efficacy, along with cybersecurity awareness and normative beliefs, positively affects

employees' intentions to comply with cybersecurity policies. In the same vein, Elifoglu et al. (2018) opined that having the relevant capability and competence in implementing security measures makes employees more likely to adhere to their organization's cybersecurity policies.

However, Belanger et al. (2017) opined that security self-efficacy does not significantly influence the intention to conform to cybersecurity policies. This result echoes findings by Kim et al. (2015) also opined that employees' higher self-efficacy does not affect intentions to comply with security policies. These differences in the effects of self-efficacy on compliance intentions may be due to differences in the sensitivity of the instruments used in these studies carried out. Belanger et al. (2017) also suggested and noted that employees with high self-efficacy might try to circumvent cybersecurity policies, resulting in a negative influence on policy compliance.

Employee stress. Organizations depend on various technologies to manage the security of their information systems available. In response to the diverse nature of security threats they face, organizations are adopting sophisticated technologies like network firewalls, document encryption technologies, network monitoring technologies, and device control technologies (Hwang & Cha, 2018). Although these technical solutions are beneficial, adopting such kinds of technologies may be stressful and challenging for employees as a whole (Hwang, & Cha, 2018). However, organizational cybersecurity goals may sometimes conflict with employees' goals, as employees may focus more on performance and efficiency objectives at hand (Hwang & Cha, 2018). Bulgurcu et al. (2010) argued and propounded that employees might choose not to

comply with cybersecurity regulations if the cost of compliance outweighs the benefits of compliance. Hwang and Cha (2018) revealed that adopting advanced technologies to improve IT adversely affected employee security policy compliance. Employees' cybersecurity compliance can only get better if you train them on using these technologies in a secure way (Yamin & Sen, 2018). Most researchers found and identified that employee stress related to cybersecurity negatively affected employees' organizational commitment and intentions to comply with security policy (Hwang & Cha, 2018; Stanton, Theofanos, Prettyman, & Furman, 2016). These findings were consistent with results from other studies that suggested and opined that employees were more stressed when faced with continuously changing technologies, resulting in adverse outcomes like dissatisfaction and decreased productivity (Lee et al., 2016a). In brief, employees may experience stress related to the use of technologies or the implementation of cybersecurity measures, and such stress can negatively influence compliance with security policies.

***Intention to comply*.** An employee's intent to comply with cybersecurity policies is his or her intention to follow recommended guidelines and safeguard their organization's information system resources from inherent potential threats (Bulgurcu et al., 2010; Mwagwabi et al., 2014). Some researchers distinguish between the intention to comply and actual compliance with security policies (Belanger et al., 2017; Bulgurcu et al., 2010). Although these constructs are distinct, intention to comply is an antecedent to actual compliance (Ajzen, 1991; Belanger et al., 2017; Bulgurcu et al., 2010).

Researchers provided literature evidence to support this (Bauer et al., 2017; Belanger et al., 2017).

Multiple factors may determine the intention to comply with cybersecurity policies. Among some factors mentioned most in the extant literature are users' self-efficacy, cybersecurity awareness, and attitude towards compliance (Kim et al., 2015; Menard et al., 2017). Some other constructs associated with intentions to comply with guidelines include normative beliefs (Belanger et al., 2017; Safa et al., 2015) and social influence (Herath & Rao, 2009). Mwagwabi et al. (2014) found threat appraisal factors like perceptions of vulnerability, threats, or severity of cybersecurity risks could influence internet users' intentions to comply with cybersecurity policies. These results were in line with Herath and Rao's (2009) findings, who suggest that the severity of impending threats may affect employees' intentions to comply with security policies.

Extrinsic determinants of compliance. An employee's intentions to comply with cybersecurity policies can also be affected by extrinsic determinants. Extrinsic behavioral determinants refer to external determinants to the individual (Safa et al., 2015). Extrinsic determinants include those that come from the organization or environments like management support or behavioral consequences such as rewards and punishment (Niblett, 2016). Pham, El-Den, and Richardson (2016) explained that rewards and sanctions are used by organizations to make their employees comply with security policies. Employees are motivated by promotions and rewards, and they could be cybersecurity policy-compliant when they get such from the management of their

organizations. Similarly, a sanction is also a strategy for enforcing cybersecurity compliance.

Management support. Management support is critical for the effectiveness of cybersecurity policy. Cybersecurity policy is the executive management team's responsibility (Rothrock, Kaplan, & Van, 2018). Without adequate stakeholder presence, the implementation of cybersecurity policies and other IT policies will not be meaningful (Alreemy et al., 2016; Flowerday & Tuyikeze, 2016). Executive management involvement and the number of capital resources invested in cybersecurity can increase cybersecurity programs' efficiency (Ifinedo, 2016; Steinbart et al., 2016). All organizational measures that enforce or implement cybersecurity policy compliance and reduce security risks start with top management support.

Application to the Applied IT Problem

Development of a security culture. Culture describes a set of shared attitudes, values, goals, and practices that characterize an institution as a whole (Dhillon, Syed, & Pedron, 2016). Hence, developing everyone's security culture in an organization is a method to mitigate security risks and enforce cybersecurity policies. Security culture development should be a top priority in every organization's agenda for a positive transformation of employees' behavior (Da Veiga & Martins, 2017). A healthy security culture is necessary to effectively implement cybersecurity policies and protect enterprise data (Dhillon et al., 2016). With the support of a company's executive management, a cybersecurity culture can exist in an organization. Though developing a security culture

takes time, cybersecurity leaders can begin by defining the security culture that fits their firms, get management support, and communicate it.

Cybersecurity management should integrate both human and technical aspects and include cybersecurity awareness, compliance, governance, audit methods, behavioral strategies, etc. (Soomro et al., 2016). When employees are not security-aware and do not have a security culture, they are not aware of inherent security risks and threats, and they cannot handle them well (Bartnes et al., 2016; Grobler, 2018). If not mitigated, cyber threats can interrupt companies' safety, maintainability, and stability by attacking their capital's confidentiality, integrity, and availability (Sallos & Garcia-Perez, 2019). Hence the need for a mature security culture. Safa, Von Solms, and Furnell (2016) opined that robust security culture develops by building standards, processes, and policies that include a training and awareness program for workers as an element of the overall business plan. One of these standards is risk management.

Risk management will help organizations access and address the gaps in their systems and enhance their security architecture and position (Joshi & Singh, 2017). Today, every bank has an implemented enterprise risk management system and information security management system to mitigate security risks and protect themselves from data and privacy breaches (Camillo, 2017). Every organization should do the same as risks affect consumers' privacy decisions (Adjerid, Peer, & Aquisiti, 2018), and enterprise risk management systems help organizations attain a mature risk culture level. Though the development of a security culture has its challenges, with communication, proactive actions, and useful security measures and enhancements, the

process can be successful (Da Veiga & Martins, 2017). Thus, consequently leading to enhanced cybersecurity policy compliance and reduced security risks.

Security awareness and policy awareness. Awareness of security and security policies are keys to mitigating security risks. Security awareness describes the employee's overall knowledge and understanding of security threats and their consequences (He & Zhang, 2019). Enhanced security awareness is crucial for every organization (Esteves, Ramalho, & De Haro, 2017). Humans are the weakest and most unpredictable link in cybersecurity (Hall, 2016; Heartfield & Loukas, 2018), And an effective counter-measure to this human factor is security awareness (He & Zhang, 2019; Nobles, 2018) and the development of a security culture (Connolly, Lang, Gathegi, & Tygar, 2017). With this strategy, the human weak-link can become less unpredictable (Horne, Maynard, & Ahmad, 2017) and a human firewall.

Security awareness is not only effective on non-technical employees but also on the technical IT professionals employees (Torten, Reaiche, & Boyle, 2018). Security awareness also mitigates the occurrence of social engineering attacks (Hatfield, 2018). Every employee should be aware that security is everyone's responsibility (Gerhold, Bartl, & Haake, 2017). Many employees still think IT is solely responsible for some technological and safety controls in their company (Hadlington, 2018). Instead of being the weakest link in cybersecurity, every employee could be a defensive security-sensitive, security-cultured, and security-compliant human firewall, serving as the first line of defense and playing the role of a security-risk whistle-blower (Mailloux, & Grimaila, 2018; Sollars, 2016).

The weak level of security awareness programs coupled with poor employee attitude and behavior all contribute to an inadequate security culture within organizational settings that can stimulate a higher and increased danger of security breaches (Ki-Aries, & Faily, 2017). Mamonov and Benbunan-Fich (2018) explained in their research on cyber threat awareness that a user's self-efficacy to protect themselves online was a factor to limit exposure and reduce threats. However, the authors found that self-efficacy alone was not an essential factor impacting a user's total awareness of impending cybersecurity threats. Ogutcu et al. (2016) suggested that relying solely on technology to protect personal or business information can lead to an increased risk of impending security breaches, particularly for those uneducated or those uncomfortable with technology. Hence the need for security awareness.

Cybersecurity policy awareness focuses mainly on understanding the cybersecurity policy requirements and the purpose of those requirements (Li et al., 2019). Cybersecurity policy awareness is different from general cybersecurity awareness. The cybersecurity policy awareness is necessary for change in behavior because a basic knowledge of an expected change in behavior is needed to carry out the behavioral change (Belanger et al., 2017). Compliance with cybersecurity policies may involve a change in user behavior. However, it is essential to understand how employees' awareness of security policies affects employee policy compliance.

Lykou, Anagnostopoulou, and Gritzalis (2019), in their study on smart airport cybersecurity, revealed that adequate policy awareness and best practices could improve day-to-day practices and create effective cybersecurity governance at airports. Molin,

Meeuwisse, Pieters, and Chorus (2018) explained that employees' perceptions of cybersecurity measures and policies enhance cybersecurity compliance and help cybersecurity managers develop a holistic security training program. However, Belanger et al. (2017) discovered that increased awareness of cybersecurity policy positively impacts overall security behavior and compliance guidelines.

Dealing with the active human connection means dealing with uncertainty as most individuals are sometimes uncomfortable or unimpressed (Aurigemma & Mattson, 2017b). Bauer and Bernroider (2017) studied the effect of cybersecurity awareness and employees' attitudes towards compliance with cybersecurity policies carefully. Both the general cybersecurity awareness and cybersecurity policy awareness significantly contributed to employees' attitudes towards compliance (Bauer & Bernroider, 2017). The attitude towards policy compliance directly affected intentions to comply (Bauer, & Bernroider, 2017). Similarly, Belanger et al. (2017) opined that awareness of security policy changes positively impacted the security policy change in a study focusing on the determinants of early conformance with cybersecurity policies.

Collaboration and knowledge sharing. Cybersecurity collaboration and knowledge sharing are closely related to cybersecurity awareness. When employees engage in collaboration and knowledge sharing with their peers, security culture is developed (Safa et al., 2016). And when all employees take cybersecurity as their responsibility, cybersecurity delivers excellent advantages (Safa et al., 2016). It is sometimes difficult to get all employees on board, but employees' participation enhances their cybersecurity awareness. When employees are informed about cybersecurity

policies and frequent training programs, their security culture can develop further (Amankwa, Loock, & Kritzinger, 2018). Knowledge sharing gotten from attending cybersecurity conferences can also help develop security culture and expertise (Shires, 2018).

A security culture model that comprises shared beliefs, values, goals, or practices communicated and practiced can offer the basics for a healthy security culture (Dhillon et al., 2016). Studies carried out have shown that Cybersecurity collaboration and knowledge sharing affect users' attitudes towards cybersecurity policies (Safa et al., 2016). Ogutcu et al. (2016) discovered that better knowledge and attitudes towards security policies are associated with less risky cybersecurity behavior (Ogutcu et al., 2016). According to Fielding (2019), mitigating cyber risks does not need to be complicated; simple mechanisms like lunch-and-learn sessions or the encouragement of knowledge sharing and collaboration of security-related issues also can help reinforce security as everyone's responsibility.

Cybersecurity training. Training employees on cybersecurity is considered an essential mechanism in managing cyber risks and employee cybersecurity policy compliance (Bartnes et al., 2016; Miranda, 2018). Education, adequate training, and high-level awareness programs are mandated in some industries to either comply with regulatory or contractual requirements bases. According to Warkentin, Johnston, Shropshire, and Barnett (2016), continuous training should occur over time. Employee training relates to employee compliance. Cybersecurity training for employees is another mechanism that organizations can use to achieve compliance.

Training may help provide a better understanding of the policies, employee compliance, security architecture, and an appreciation of the importance of securing organizational cybersecurity assets. Galinec, Možnik, and Guberina (2017) also opined that these cyber defense strategies protect the cyberspace at the national level.

Ayyagari and Figueroa (2017) opined that cybersecurity policy training was more effective when it involved showing employees the impact of employee cybersecurity policy noncompliance, rather than just presenting the stipulated requirements. It is crucial to provide employees the reasons behind written security policies (Ayyagari & Figueroa, 2017). The Cybersecurity managers can use isomorphism to establish new training programs as part of their overall Cybersecurity plan (McGovern, Small, & Hicks, 2017). Security training is practical when done in an open environment of trust and good culture (Andrews-Speed, 2016). Though there is no particular standard for cybersecurity education, training, and awareness programs, cybersecurity managers must create a uniform strategy and security culture that motivates sufficient training.

Regulations vary due to differences in the industry. As a result, firms that offer cybersecurity services to different industries have a challenge (Curran, 2015), and their cybersecurity managers also have challenges. However, they strive to create cybersecurity policies to increase security awareness on security risks and manage cybersecurity (De Bruijn & Janssen, 2017). Cybersecurity managers must know the definition of cybersecurity education, cybersecurity training, and cybersecurity awareness (Torten et al., 2018). Cybersecurity education combines passive and active

instruction to enhance the employee's overall security skill level. The cybersecurity training can occur with standard passive testing techniques, and cybersecurity awareness could be gotten through dialogue and collaboration in the form of personal experience to change cybersecurity behavior (Curran, 2015).

The combination of cybersecurity education, training, and awareness should be part of any cohesive cybersecurity strategy (Mamonov, & Benbunan-Fich, 2018). Employees should be educated on the varieties of threats and risks that exist, trained on recognizing and mitigating, and being constantly aware of the security landscape around them (Sollars, 2016). The required specified training should be as needed, but the general cybersecurity training and awareness should be updated regularly and should be done according to pattern and regularly, according to company policy.

Targeted training transcends gender (Park et al., 2017a). Targeted training also transcends age. Anwar et al. (2017) revealed that older employees possess a more robust perception of cybersecurity than young workers. In the same vein, Yan et al. (2018) also showed that women are more security-conscious and privacy-conscious than men. Park et al. (2017a) researched health information security awareness using nursing studies as a case study. Park et al. (2017a) suggested that nursing students are tempted not to comply with the Health Insurance Portability and Accountability Act because of their exposure to patients' data during their internship. And simultaneously, they developed personal values and beliefs or perceptions regarding the importance of health information privacies (Park et al., 2017a).

The observed nurses suffered from improper, inadequate, or non-existent training (Park et al., 2017a). Park et al. (2017a) explored how an individual's behavior can be influenced by adequate training utilizing a cybersecurity framework and found out that security awareness positively influences the students' cybersecurity compliance. The study proved that cybersecurity training could help deter improper behavior and help comply with security policies and regulations. Park et al. (2017a) opined that cybersecurity awareness does have different levels: being generally aware, having a comprehensive understanding, learning explicitly by training, and unconsciously by patterned behavior. They also explained that this security awareness could significantly influence personal behavior and compliance. Park et al. (2017a) opined that health care professionals are not unique in their needs when it comes to cybersecurity management.

The manner an employee perceives the necessity of cybersecurity depends on how well they comply with cybersecurity policies and procedures (Kearney & Kruger, 2016). Developing a cybersecurity strategy that incorporates the importance of cybersecurity built on trust within the organizational setting are seeds for a healthy and active security culture where users believe the environment is secure effectively (Elkhannoubi & Belasissaoui, 2016; Kearney & Kruger, 2016). The training programs that include organization-wide cooperation, coordination, and technical expertise can help strengthen its overall cybersecurity operations (Bartnes et al., 2016). The more computer savvy users and are familiar with impending security threats that may exist online are likely to exercise better computer security habits than those unknowledgeable with imminent threats (Jeske & Van Schaik, 2017).

The cybersecurity managers can benefit from using a quick survey of their employees to see who fits into two categories before developing adequate training and high-level awareness programs. The study may quickly identify those with advanced cybersecurity knowledge and skills who could offer a significant compliance prediction (Jeske & Van Schaik, 2017). The survey may have bias depending on the population and the questions asked.

The skills assessment is not easily measured. Kearney and Kruger (2016) suggested that employees with advanced cybersecurity knowledge and skills are susceptible to showing personal and confidential information contents. However, McCormac et al. (2017) discovered that individuals with a higher perceived cybersecurity awareness IQ are more compliant than those with lower cybersecurity awareness IQ (McCormac et al., 2017). Increasing cybersecurity awareness IQ should start with targeted training that is consistent and continuous. The targeted training can help build a healthy cybersecurity culture. A comprehensive cybersecurity training program should avoid a generic, one-size-fits-all approach. Instead, the training and awareness programs should be specific to individuals depending on their needs and industry requirements.

Curran (2015) designed and outlined a framework that can be used on an annual basis by Cybersecurity managers to develop a training program. However, Safa et al. (2016) recommended frequent training as opposed to yearly training. Curran (2015) also revealed four principles for planning a cybersecurity program. He recommended a training program for educating the employees on cybersecurity; communicating the

management's commitment to the training; communicating the regulatory and organizational compliance policies, and developing and relating the penalty for non-compliance (Curran, 2015). Similarly, Bauer et al. (2017) recommended using videos showing the risk and threats associated with cybersecurity.

Cybersecurity managers should use a deterrent mentality and videos that show consequences to inherent security risks and threats. They should also develop realistic metrics that can be applied to evaluate and correct awareness and training methods. The manager should offer workers mechanisms to provide inputs on the program, allowing for constant improvement and conclusively. Lastly, Bauer et al. (2017) suggested that they should customize adequate security training and awareness programs based on the user's differences, such as location, skill level, and responsibility areas. Flowerday and Tuyikeze (2016) conducted a risk assessment for a company and recommended developing training programs to ensure security policy compliance (Flowerday & Tuyikeze, 2016). Hence training can help reduce security risk and enforce cybersecurity policy compliance.

Conceptual Framework: Theory of Planned Behavior

The framework for this research is TPB. TPB implies that behavioral intention can predict an individual's attitude towards the behavior, perceived behavioral control, and subjective norms (Ajzen, 1991; Sommestad et al., 2019). In other words, the TPB explains these three factors that determine an individual's intention to perform a behavior. Table 2 shows the three primary constructs and the two other factors, intention and behavior. Ajzen (1991) postulated TPB based on the premise of the TRA (Fishbein &

Ajzen, 1975), which he broadened to explain human behavior in particular contexts. Around 1975, Fishbein and Ajzen (1975) nurtured the TRA to demonstrate new technology adoption. Ajzen (1991) used the TRA as a pivot to develop the TPB, which applies behavior as an indicator of technology adoption.

Table 2

Constructs of the Theory of Planned Behavior

Constructs	Description
Attitude towards behavior	The extent to which one appraises a behavior as favorable or unfavorable
Subjective norms	The perceived belief of individual from social pressure to do or not do a specific behavior
Perceived Behavioral Control	Individual perception of his ability or inability to do an activity
Intention	The indication of an individual's readiness to do a behavior.
Behavior	The outcome of intention and actual behavioral control

TPB is a theory that emanated due to TRA's limitations in addressing a person's behavior over which he or she has no full volitional control (Ajzen, 1991). TPB was postulated by Ajzen (1991) in other to address the weakness of the TRA. Though TPB is not a theory of behavior change, TPB does help describe and predict people's behavior and intentions (Ajzen, 2014). The perceived behavioral control joined with attitude, and subjective norms combine to form intention resulting in a particular attitude (Ajzen, 1991). When control is missing in a given situation, it is less likely that someone will perform a given action (Madden, Ellen, & Ajzen, 1992). Behavior can improve by allowing a cybersecurity manager to have more control over a given situation. Training and awareness is a tool of a cybersecurity manager.

Attitude toward behavior and applications. Attitude towards a behavior refers to an individual's appraisal of a behavior or the extent to which someone evaluates a favorable or unfavorable behavior. Ajzen (1991) opined that attitude towards a behavior gets influenced by information about the behavior or beliefs about the behavior. Attitude towards the behavior is one of the two significant constructs extracted from TRA. Ajzen (1991) explained that Attitude toward behavior as an encouraging or discouraging appraisal a person holds about a specific behavior. The salient behavioral beliefs of the person affect the construct (Armitage & Conner, 2001). Persons connect these beliefs to specific results of doing a behavior. The person sees these results as good or bad, so an attitude toward the behavior is perfected (Lee et al., 2016a).

Attitude describes a more significant part of the intended behavior implemented (Arpaci & Baloglu, 2016; Flores & Ekstedt, 2016; Jafarkarimi, Saadatdoost, Sim, & Hee, 2016; Safa et al., 2016). Attitude can also be affected by the education intended to change this attitude (Li et al., 2019). Organizational narcissism, perceived vulnerability, perceived severity, and reward are determinants of Attitude towards a behavior (Cox, 2012). Mayer, Gerber, McDermott, Volkamer, and Vogt (2017), however, digressed and viewed reward as bad for security compliance.

Attitude has a high effect on intention in TPB (Ajzen, 1991). Lebek, Uffen, Neumann, Hohler, and Breitner (2014) highlighted that 80% of IT studies applying TPB showed strong correlations between attitude and intention, with sixty respondents indicating significant relationships at $p < 0.01$ level. Hofeditz, Nienaber, Dysvik, and Schewe (2017) found out that behavior attitude was more significant than the subjective

norms and perceived behavioral control. Results of studies show attitude is the dominant predictor of intention. While some different results from another study revealed that attitude is the least significant predictor of intention (Donald, Cooper, & Conchie, 2014).

On applying TPB to social networking ethics, Jafarkarimi et al. (2016) reported that Attitude to Behavior is much more significant than perceived behavioral control and more significant than the subjective norms. In the study conducted by Dang-Pham, Pittayachawan, and Bruno (2017) on sharing information security knowledge, the behavior attitude was also more significant than the subjective norms, though perceived behavioral control was found insignificant. In the same vein, the attitude was also more significant than subjective norms and perceived behavioral control in Gurung and Raja's (2016) study on online privacy and security.

Mayer et al. (2017) also researched security and productivity and discovered that Attitude towards behavior is the most significant, followed by subjective norms and perceived behavioral control. Koohikamali, Peak, and Prybutok (2017) researched disclosure of information on social media among the users and revealed that attitude towards behavior was the most significant factor, while the subjective norms were insignificant. Bauer and Bernroider (2017) found attitude to behavior significant in their study on cybersecurity awareness. Park, Hsieh, and Lee (2017b) and Heetae, Hwansoo, and Hangjung (2017) also revealed that attitude to behavior is the most significant, followed by subjective norms and perceived behavioral control.

Subject norms and application. The subjective norm is the other construct taken from TRA. Subjective norms represent the individual’s social pressure to do or not do a

specific behavior (Ajzen, 1991; Yazdanmehr & Wang, 2016). Most times, subjective norms have to do with an individual's perception of social pressure to do or not do a behavior (Ajzen, 1991). Armitage and Conner (2001) explained that important normative beliefs of a person affect the subjective norms. In other words, normative beliefs are factors affecting subjective norms. A person can transfer data during knowledge sharing in a company (Dang-Pham et al., 2017). The information is also communicable through the company's cybersecurity policies and security measures (Soomro et al., 2016). Assuming the person believes that other persons feel they should or should not perform, it will have a good or bad impact on the individual's intention to do the behavior (Armitage & Conner, 2001; Yazdanmehr & Wang, 2016).

Jafarkarimi et al. (2016) assumed that subjective norm is a weak cybersecurity compliance predictor. Some studies reveal that subjective norm is an effective cybersecurity compliance predictor (Hu, Hu, Wei, & Hsu, 2016; Yazdanmehr & Wang, 2016). Sher, Talley, Yang, and Kuo (2017) supported the motion that subjective norm is the most significant predictor after research on hospital employees and medical records' privacy. Bauer and Bernroider (2017) also found the subjective norms significant while they found that perceived behavioral control insignificant. Some research works that are not IT-related follow this approach. A research work concluded that subjective norm is the most significant predictor of intention (Prapavessis, Gaston, & DeJesus, 2015).

The significance of applying subjective norms in detecting intended behavior is a subject of contention. Armitage and Conner (2001) assumed that the subjective norm is the weakest predictor after reviewing 161 research works that applied TPB. However, the

researchers explained that it could still be useful when many measures were applied using the construct and other empirical evidence (Armitage & Conner, 2001). Donald et al. (2014) revealed that the subjective norms to be the second-best predictor of TPB. Cox (2012) also took the subjective norms to be the best construct of intended behavior.

Lebek et al. (2014) explained that subjective norms have a statistical impact on intention in 75% of the studies, after reviewing some IT studies that applied TPB. Some other research works that were not conducted solely on TPB have applied subjective norms in their frameworks and discovered that it is an efficient predictor of intention (Tsai et al., 2016). While other research works assumed subjective norms was a weak predictor of intention (Arpaci & Baloglu, 2016; Cheng, Li, Li, Holm, & Zhai, 2013). Conflicts exist using the construct. However, the conflicts are okay for as long as the requirements set by Ajzen (1991) are satisfied in their study.

Perceived behavioral control and applications. Perceived behavioral control refers to the level to which an individual sees a specific behavior as easy or challenging to perform (Ajzen, 1991). Perceived behavioral control is an individual's perception of how easy or hard it is for him to do an activity (Moody, Siponen, & Pahnila, 2018). Locus of control and Self-efficacy are often constructs of Perceived Behavioral Control (Ifinedo, 2014; Jansen & Van Schaik, 2017). Suppose there is a perception that an easy to do behavior enhances employee cybersecurity policy compliance. In that case, it can benefit cybersecurity managers to study and apply TRA and TPB as they develop training and awareness programs. An individual's behavior can be heavily influenced by their self-efficacy to perform and control action, reasoning that more training and awareness

will improve Cybersecurity compliance. The TRA, the behavioral intention in TPB, remains a vital tenet of the theory.

Perceived behavioral control is also affected by experience and anticipated obstacles to completing the behavior (Ajzen, 1991). Therefore, the concept of perceived behavioral control is compatible with the idea of perceived self-efficacy put forth by Bandura (1989). Perceived behavioral control differentiates the TPB from the TRA, which describes behavioral intention concerning attitude towards behavior and subjective norms only (Ajzen, 1991). The TPB proposes that perceived behavioral control may also be applied directly to predict actual behavior.

Ajzen (1991) suggested that increased behavioral control has a higher likelihood of more effort to accomplish a behavior. According to Ajzen, individuals who have high confidence in performing a task will persevere more than individuals who doubt their skills. Also, Ajzen (1991) opined that perceived behavioral control could measure actual behavioral control, which can predict actual behavior. TPB explained that an individual's intention to act after being given actual control of the behavior will lead to the occurrence of the actual behavior (Aurigemma & Mattson, 2017a). An estimation of behavioral control is solely dependent on perceptions (Ajzen, 1991). The study of Mahmood, Dahlan, Hussin, and Ahmad (2016) also revealed TPB as a predictor of behaviors.

Ajzen (1991) explained the importance of including perceived behavioral control in the framework to justify involuntary behaviors. This variable sometimes includes the factors of locus of control and self-efficacy (Ifinedo, 2014). Perceived behavioral control explains a person's belief that he is in a position to perform and technically do so (Cox,

2012). Jiang, Ling, Feng, Wang, and Guo (2017) did a study and found out that perceived behavioral control was more significant than Attitude to Behavior and subjective norms.

Intention. TPB explains people's intentions to perform certain behaviors. In other words, TPB describes intention as their readiness to do a particular behavior (Ajzen, 1991; Ajzen, 2011; D'Arcy & Lowry, 2017). Intentions mainly refer to motivations that influence behavior and indicate how much effort people are willing and able to put into performing a specific behavior (Ajzen, 1991). In general terms, a proposed firm intention to perform a behavior should correlate with a higher likelihood of performing the behavior (Ajzen, 1991). Therefore, a behavioral intention can be translated or interpreted into an actual performance of the behavior only if the person can decide whether to perform the behavior or not (Ajzen, 1991). Additionally, intention, behavioral control, and behavior's performance depend on the availability of resources, the ability to perform the behavior, or others' cooperation (Ajzen, 1991). Barton, Tejay, Lane, and Terrell (2016) and Safa et al. (2016) also opined that normative beliefs influence a person's intentions and actions. The strong relationship between intention and behavior applies to Cybersecurity policy compliance (D'Arcy & Lowry, 2017; Lebek et al., 2014). Moreover, TPB has always been a strong predictor of cybersecurity compliance (Sommestad, Karlzen, & Hallberg, 2015). Lebek et al. (2014) considered TPB as the most common theory applicable to cybersecurity.

Background factors of theory of planned behavior. In addition to the three central constructs in the TPB, other factors may interact with the main factors to affect behavioral intention. According to the TPB, the three factors discussed might not be the

only factors affecting behavior (Ajzen & Albarracin, 2007). Other background factors may also influence behavior indirectly. Background factors entail factors that differ among individuals, like experience, demographics, disposition, or knowledge (Ajzen & Albarracin, 2007). The TPB fathers explained that background factors like knowledge, social context, and personality have a significant impact on the predicting factors (Sommestad, 2018).

Background factors may indirectly affect behavioral intention by shaping behavioral, normative, and control beliefs (Ajzen & Albarracin, 2007; Samhan, 2017). Conner, McEachan, Taylor, O'Hara, and Lawton (2015) explained that affective determinants and individual differences could impact the TPB components. The background factor may play an indirect role. In his study on cyber risk management insurance and healthcare providers' intentions to resist electronic medical records, Samhan (2017) used information security awareness as a background factor that impacts the creation of resultant beliefs about the Electronic Medical Record system.

Limitations of the Theory of Planned Behavior

Despite all the excellent benefits and applications of TPB, it has shortcomings, just like every other framework (Zhang, 2018). TPB can't explain some social behaviors. Sommestad (2018) studied work-related groups and information security policy compliance and found out that TPB could not account for some factors. Sommestad et al. (2019) also did a study and had to extend TPB's limits by applying the framework to habit and regret. Zhang (2018) demonstrated that TPB does not predict complaints on products. Neither does it account for economic factors.

Zhang (2018) further explained that TPB's significant limitation is that it does not account for factors such as fear, threats, and mood. Though the mood factor is not inclusive in TPB, mood can influence subjective norms, attitudes toward behavior, intention, and perceived behavior control and intention (Zhang, 2018). Brase, Vasserman, and Hsu (2017) revealed that mental models also affect cybersecurity behavior. Zhang (2018) explained that an individual with a negative mood has an attitude that relates closes to intention, and an individual with a positive mood has subjective norms that relate closely to intention. Zhang (2018) also related the negative and positive mood to health and how its behavior affected the health and explained that positive and negative mood should be a factor in predicting behavior.

Zhang (2018) explained that TPB is limited to the rational behavior of an individual. Zhang (2018) opined that no human behavior could exist without emotion. Therefore TPB is limited for not explaining individual behavior related to feeling (Zhang, 2018). Zhang (2018) suggested that the future TPB model should be able to give an explanation of human behavior concerning emotion. Also, Zhang (2018). also opined that TPB gives no account for culture and differences in individuals and contexts and recommends that the future TPB model include culture, individual differences, and settings.

Analysis of Competing Theories that Support the Theory of Planned Behavior

Theory of reasoned action. The TRA is closely related to TPB, emanating from psychology. TRA got initially created by Fishbein (1967) and then expanded by Fishbein and Ajzen (1975). TRA tends to be applicable when an action or behavior is under an

individual's conscious (habit) control (Madden et al., 1992). But when actions or behaviors are unconscious and not habitual, TPB is considered more useful. TRA's usefulness indicates that an individual's behavior is motivated by his behavioral intention and vice-versa. TRA shows that intention is a direct factor of behavior, and it is motivated by the attitude towards doing the behavior and social pressures to do a given behavior (Sharma, Al-Badi, Govindaluri, & Al-Kharusi, 2016). TRA acknowledges the attitude and the behavioral intention of a person. TPB is also applicable as a predictor of a person's action under some circumstances (Paul, Modi, & Patel, 2016).

Intention and attitude imply control over conscious behavior and are limitations of TRA (Ajzen, 1991). However, both of them are useful. Both factors can be applied to cybersecurity, thereby producing an atmosphere where personal behavior is conscious and more certain through training and awareness. Intention and attitude also motivate the examination of TRA by cybersecurity managers. Kim et al. (2015) explored behavioral factors influencing employee cybersecurity policy compliance, using the TRA as a framework and discovered that attitude towards compliance, beliefs, and self-efficacy impacts compliance.

The process of applying the TPB shows that an individual's behavior is motivated by the person's attitude toward the behavior and the subjective norms regarding the given behavior's performance. Lee, Li, Shin, and Kwon (2016b) explained that TPB is defined by evaluating an individual's belief as a result of behavior and how easily the behavior is implementable. TPB is a better theory than TRA because TRA is limited in tackling a person's behavior over which he or she has no full volitional control (Ajzen, 1991). This

inclusion improved the predictability of TPB's compliance intention (Sommestad et al., 2015) and made TPB a more suitable theory for this study.

Protection motivation theory. Protection motivation theory (PMT) is another theory that competes with TPB. The theory is also applicable in the field of cybersecurity compliance research. The theory got created by R.W Rogers in 1975 (Rogers, 1975). PMT is a compulsive social communication model based on fear and has grown to a more generalized theory regarding persuasion, especially in health benefits studies that are carried out (Sommestad et al., 2015). PMT is a framework applied to describe how fear motivates cybersecurity policy compliance (Pham et al., 2016).

PMT seeks to impact attitudes, behaviors, cognition, and behavioral intention (Pham et al., 2016). Jansen and Van Schaik (2017) opined that PMT is useful for explaining the behavior of users. Thompson, McGill, and Wang (2017) explained that PMT is suitable for analyzing individual behaviors such as end-users' behavior when encountering a risky situation or dicey event. Rajab and Eydgahi (2019) concluded, in their study on the intention to comply with cybersecurity policies in higher education, that PMT is the best predictive framework for intentions to comply because of the impact of three of its core predictors of perceived vulnerability, response efficacy, and response cost.

While Anwar et al. (2017) describe PMT as a theory that concentrates on a person's intention to secure themselves based on what they perceive to be a threat (Anwar et al., 2017). The framework consists of motivational factors that fall into threat appraisals or coping appraisals category (Posey, Roberts, & Lowry, 2015; Tsai et al.,

2016). In the threat appraisals, this category is the factor of perceived vulnerability and perceived severity (Crossler, Long, Loraas, & Trinkle, 2014). The theory relates to the individual's perception of how susceptible they are to vulnerability and how severe the vulnerability results should be realized (Arachchilage, Love, & Beznosov, 2016). The other category of coping appraisals comprised response cost, response efficacy, and self-efficacy (Crossler et al., 2014). This set addresses the individual's ability to take preventive action, how powerful the effect will be, and what effort level will be required (Posey et al., 2015; Sommestad et al., 2015). The motivational factors here share similarities in terminology and meaning to like terms in the field of cybersecurity. There is presumed relevance of the application of PMT to the area of study.

The PMT gives room for a set of essential stimulus variables that interplay in fear appeal and explains the cognitive processes which mediate an individual's acceptance of suggested sets of actions or recommendations in a fear appeal scenario (Rogers, 1975). Fear appeal refers to the contents of communications that describe unfavorable consequences that can occur if a specific set of recommendations is not followed (Rogers, 1975). Concerning PMT, there are majorly three stimuli variables in a fear appeal, namely: the level of noxiousness of a specific event, the probability that the given event will occur, and the effectiveness of a coping response that may counter the noxious stimulus.

Rogers (1975) opined that the three variables in a fear appeal initiate cognitive processes. These processes are applied to evaluate communicated information regarding noxiousness, the probability of occurrence, and the efficacy of the coping responses to

the event (Rogers, 1975). The theory is that the cognitive processes whereby appraising a fear appeal are responses to environmental stimuli that have also been received by the individual processing the fear appeal. Rogers (1975) opined that the cognitive processes affect an individual's attitude by arousing a protection motivation, and the amount of resultant protection motivation will or will determine the intention of the individual to comply with communicated recommendations. Summarily, the PMT assertion states that protection motivation arises from the assessment of an event as unpleasant and likely to occur and the belief that responding with recommended actions may prevent the incident from happening.

Herath and Rao (2009) used PMT in their study on cybersecurity behavior. In this perspective, security threats are harmful, and security policies are the recommended solutions that cybersecurity managers can use to deal with the risks. Individuals can find security policies useful based on their beliefs of how effective the policies are against security threats (Herath & Rao, 2009). Their study's outcomes showed that employees' perceptions about the severity of a security breach, response efficacy, and self-efficacy had a positive effect on their attitudes towards compliance with cybersecurity policies (Herath & Rao, 2009).

Adhikari and Panda (2018) conducted a study on users' information privacy concerns and privacy protection behaviors in social networks, intending to know the influence of antecedents of users' information privacy concerns on media privacy protection behavior. The researchers utilized the Social Cognitive Theory and PMT and analyzed the research framework with structural equation modeling. The results of the

study of Adhikari and Panda (2018) show that perceived vulnerability, perceived severity, and self-efficacy significantly affect user information privacy concerns and privacy. The PMT has also been applied to give deep insight into behavioral change in cybersecurity (Hanus & Wu, 2016; Menard et al., 2017; Tsai et al., 2016). The PMT also beams searchlight on attitude change based on fear appeal and explores a limited set of components and cognitive processes that may affect persuasion (Rogers, 1975).

Jansen and Van Schaik (2017) applied hybrid models comprising PMT and TPB to evaluate intentions to utilize online banking. The researchers dissected Subjective norms into injunctive norms and descriptive norms. While the descriptive norms are similar in definition as normative beliefs and were significant, the Injunctive norms were not significant. They dissected Perceived Behavioral Control into self-efficacy and locus of control. Anwar et al. (2017) studied gender differences and employee cybersecurity behaviors using PMT. They compared the cybersecurity behavior model's constructs, testing male and female employees in their survey research. A statistically clear gender-wise difference in IT skills, cues-to-action, old experience, security self-efficacy, and cybersecurity behavior got observed. The self-efficacy of women was lower than that of men. Therefore the researchers recommended that women should have specialized training. Anwar et al. (2017) suggested that the studies' results could motivate creating cybersecurity training that is gender-specific to enhance employees' behaviors and attitudes.

PMT is the sole primary competitor to TPB in the extant research but is also complementary in practice, and researchers often combine the two frameworks

(Sommestad et al., 2015). PMT's insufficiency got tackled in TPB through the subjective norms construct and related informal sanctions (Cheng et al., 2013). These put TPB as a recognized and a better theory for this research.

General deterrence theory. General deterrence theory (GDT) is a framework utilized in many cybersecurity studies to explore why employees comply or don't comply with their companies' cybersecurity policies. The GDT emanated from the study of criminology (Pham et al., 2016). GDT was founded by Gibbs forty-six years ago (Moody et al., 2018). Chen, Wu, Chen, and Teng (2018b) opined that GDT is the most cited theoretical framework in information security literature.

In comparison, Lebek et al. (2014) explained that GDT is the second most applied theory in end-user cybersecurity compliance research. GDT opines that individuals consider how likely they will receive punishment if they get arrested while performing an illegal act and how severe the penalty will be (Cheng et al., 2013). Moody et al. (2018) opined that the theory's core tenet is that individuals get involved in crimes because the benefits surpass the cost.

Park et al. (2017a) applied the GDT concerning education and training on nursing students, and the outcome was positive. The focus on the consequences of bad behavior practice enhanced the security awareness and compliance of the nursing students (Park et al., 2017a). Aurigemma and Mattson (2017a) conducted a study on deterrence and punishment experience impacts on ISP compliance attitudes and used GDT to explore sanction effects on the employees' behavioral intention. Pham et al. (2016) opined that rewards and penalties were applied to make employees comply with security policies.

However, the researchers explained that sometimes, sanctions and rewards do not impact the implementation of cybersecurity compliance (Pham et al., 2016). TPB is much broader than GDT, which focuses more on punishment. Therefore, TPB, which has more motivational considerations, is more considerable for this study.

Rational choice theory. RCT is another framework that emanated from criminology. The RCT comprises the factors of formal and informal sanctions (Shepherd & Mejias, 2016). The RCT framework was created by Becker 52 years ago (Kim & Han, 2019; Moody et al., 2018). The core proposition is that individuals who break the law evaluate the benefits and costs of such behavior to determine if they want to break the law (Kim & Han, 2019). Kim and Han (2019) explained that people behave based on the cost and benefits of the consequences of doing a given behavior. Kim and Han (2019) used the framework in their study on a corporate social responsibility perspective of employee cybersecurity policy compliance to explore perceived costs and benefits. RCT is an excellent framework for research on cybersecurity policy compliance. The RCT is a rationality-based behavioral theory, just like TPB.

RCT focuses mainly on the individual perception of cost and benefit. Hence RCT based research on security policy compliance is based on the costs and benefits of compliance (D'Arcy & Lowry, 2017). D'Arcy and Lowry (2017) and Chen et al. (2018b) also explained that several studies had utilized RCT constructs such as perceived costs, perceived benefits, rewards, sanctions, and risks to get their findings. However, some researchers combine RCT with other rationality-based behavioral theories to get a more comprehensive model that will focus on the cost and benefits of security policy

compliance and behavioral performance (Bulgurcu et al., 2010). D'Arcy and Lowry (2017), in their study on employee cybersecurity policy compliance, utilized a multilevel RCT and TPB based model and discovered that beliefs forecasted information security policy compliance with affective determinants and everyday workplace behaviors and events. Selecting TPB with subjective norms is more suitable for this research because it is much broader and has more motivational factors.

Social cognitive theory. The SCT also emanated from psychology. The theory got created by Bandura (1989). SCT has three determinants related to environmental expectations and self-efficacy and outcomes (Font, Garay, & Jones, 2016). Bandura (1989) opined that affective and cognitive determinants mix with environmental factors to decide human beings' behavior. The core construct in SCT is the factor of self-efficacy. Self-efficacy relates to a person's belief, perseverance, ability, and motivation (Bandura, 1989). Self-efficacy impacts the cognitive, motivational, and affective activities of individuals. Self-efficacy impacts cognitive activities by affecting the individual assessment of capabilities (Bandura, 1989). Self-efficacy impacts affective activities because the motivation level, stress level, and emotions are also affected (Bandura, 1989). People with higher levels of self-efficacy handle stress in a better manner. Self-efficacy is the degree of motivation and effort utilized in an activity (Bandura, 1989). SCT is closely related to the TPB framework. However, for this particular research, the researcher didn't apply the SCT framework. The TPB's subjective norms, attitude to behavior, and perceived behavioral control make it a preferable choice for this research.

Analysis of Competing Theories that Contrast the Theory of Planned Behavior

Technology acceptance model. The TAM was postulated and propounded by Davis (1989) to predict and explain technology systems' use. TAM's main primary constructs are perceived usefulness and ease of use, with two fundamental system use determinants. The theory is closely related to TRA and is widely applied in IT research (Mortenson & Vidgen, 2016). The TAM was a natural progression from the TRA and TPB. TAM's use combined perceived ease of use and perceived usefulness as drivers toward business intelligence and, ultimately, technology adoption (Shiau & Chau, 2016). TAM mostly uses the independent variable of attitude as the predictor of behavior intention with the same definition and meaning as TRA. The disparity between the two frameworks is the use of the perceived ease of use and perceived usefulness as motivational factors that affect attitude (Davis, 1989). TAM will not be acceptable for this study because focusing solely on attitude will be an obvious limitation.

The perceived notion of usefulness is a measure of the extent to which people believe an application will help them perform their job (Davis, 1989). Therefore, a system is regarded as highly useful if the user thinks there is a positive relationship between system usage and performance (Davis, 1989). Also, perceived ease of use is an individual's belief of how much the system's use is free of effort (Davis, 1989). Davis believed that an application that is perceived to be easier to use is more likely to be accepted. Davis (1989) stressed that perceived ease of use is similar to Bandura's (1989) self-efficacy construct.

In the context of behavioral cybersecurity, the TAM opines that two factors can solely be predicting an individual's intentions to comply with cybersecurity policies. These significant factors are the extent to which they perceive compliance with the policy as useful and the perceived ease of use of security measures (Lebek et al., 2014). This view purely assumes that cybersecurity policies are systems, and compliance with policies is system use. However, Davis (1989) applied the model to technology, systems, and applications rather than policies. TPB will be better for the study because the focus is on policy compliance rather than technology and systems.

Institutional theory. Institutional theory is another theory that competes with TPB in cybersecurity policy compliance amongst other areas of study. The theory got created by Paul J. DiMaggio and Walter W. Powell in 1983 (DiMaggio & Powell, 1983). The theory is a rival theory of TPB. The institutional theory uses four primary dependent constructs, including institutional adoptions, change, isomorphism, and conformity (Scott, 1987). The secondary independent constructs can develop policies, practices, and norms (DiMaggio & Powell, 1983). The theory tends to become a global approach (Scott & Amarante, 2016).

The theory creates guidelines for social behavior within organizations from the processes that establish structures such as practices, frameworks, or routines (Lopes & Sá-Soares, 2014). The institutional theory also supports studies on the implementation of cybersecurity policies in an organization, as it explores the subject matter explicitly and imparts a better understanding of the role of organizational goals, cultural factors, and human factors in policy compliance and policy implementation. Lopes and Sá-Soares

(2014) used the institutional theory as a framework when they researched establishing strategies to improve the adoption of policies on information systems security.

Cybersecurity leaders' strategies could originate from institutional environmental factors like culture, behavior, and regulatory requirements (Sherer, Meyerhoefer, & Peng, 2016). Cardinale (2018) opined that being employed in an institution could enable an employee to resolve issues, do well, and be very efficient. According to Angst, Block, D'Arcy, and Kelley (2017), Institutional theory is also applicable in comparing symbolic and substantive adoption of actions or policies. Andrews-Speed (2016) listed three different types of change associated with institutionalism concepts. He listed them as Layering, which has to do with enhancing existing procedures and processes; Conversion, which includes new goals to change the institution's entire role, and; Drift, that happens when there is negligence in policy compliance gradually takes effect. Cybersecurity managers must understand that there is a higher chance for acceptance and compliance when change management is handled transparently (Andrews-Speed, 2016).

Schilke (2018) opined that environmental pressures influence an organization and that cybersecurity managers should know the effect of uncertainty in aligning with the environment's demands. Takahashi and Sander (2017) also explained that the institutional environmental factors' results might be affected by societal determinants like social and cultural determinants. Mohamed (2017) opined that the institutional theory also emphasizes the institution at the macro level than on the individual's influence. These demerits of institutional theory give TPB an advantage over it.

Similar Studies that have used the Theory of Planned Behavior

TPB is applicable as a theoretical framework in behavioral sciences as well as cybersecurity compliance studies. Sommestad et al. (2019) made some adjustments and extensions of TPB by applying the framework to habit and regret in their study on TPB and information security policy compliance. After collecting 645 valid questionnaires from 645 participants, they discovered that some of the variables had to do with habit and regret, and the two factors enhanced the predictions of TPB (Sommestad et al., 2019). Sommestad et al. (2019) discovered that habit enhanced explanatory power. The researchers opined that further studies are needful on the relationship between habit and intention. The trio discovered that the added explanatory power for anticipated regret and habit were significant. The values of the adjusted explained variance for the two factors were $\Delta\overline{R}\ 2 = 3.4$ and $\Delta\overline{R}\ 2 = 2.6$, respectively (Sommestad et al., 2019). On closer examination of the points, Sommestad et al. (2019) opined that habit is not a direct intention's causal antecedent based on points. The researchers explained this might have been due to dynamic information systems and efforts to limit old behavior's impact. Sommestad et al. (2019) opined that anticipated regret, therefore, is the only factor that could extend TPB. The study of Sommestad et al. (2019) was also on information security policy compliance, just like this study. However, in contrast to this study, the research of Sommestad et al. (2019) is a quantitative and survey research that was conducted in Sweden and with 645 participants.

According to Ajzen (2011), normative influences do not have only subjective norms. They also include descriptive norms. While subjective norms have to do with the

extent to which paid workers believe that the management expects them to comply with the cybersecurity policies, descriptive norms have to do with the extent to which paid workers believe the management are behaviorally complying with the cybersecurity policies (Herath & Rao, 2009). Herath and Rao (2009) explained that descriptive norms are not very common in cybersecurity policy compliance publications (Herath & Rao, 2009). This lack of popularity of descriptive norms prompted cybersecurity scholars like Bauer and Bernroider (2017) and Yazdanmehr and Wang (2016) to call for more mentions in the context. Flores and Ekstedt (2016) used normative beliefs as a predictor in their study. Aurigemma and Mattson (2017b) researched utilizing eight TPB models and explained employee status as a determinant of cybersecurity compliance. In contrast to this research, Aurigemma and Mattson (2017b) research is a quantitative and survey research in a US university and 227 participants from Asia, Europe, Middle-east, and North-America.

Snyman and Kruger (2017) conducted studies on applying behavioral thresholds to analyze collective behavior in information security and applied TPB. The result was promising and the method used was suitable for measuring, analyzing, and predicting security behavior and awareness (Snyman & Kruger, 2017). The study of Snyman and Kruger (2017) was also on cybersecurity behavior. However, in contrast to this study, Snyman and Kruger's (2017) research was quantitative and survey research conducted in a South African university and 22 participants. Moody et al. (2018) studied a unified model for information security policy compliance using TPB and ten other frameworks. The researcher’s unified model successfully did an empirical examination of the degree

to which information security frameworks are empirically similar and how the contrasting theories can complement each other (Moody et al. (2018). The study of Moody et al. (2018) is also on security policy compliance. However, in contrast to this study, the research of Moody et al. (2018) is a quantitative and survey research that was conducted in a university in Finland with 178 respondents.

Hina, Selvam, and Lowry (2019) also did a study using TPB. The researchers conducted a study on Institutional governance and protection motivation (using TPB and self-efficacy from PMT) with a focus on employees' security compliance behavior in higher education institutions located in third world countries (Hina et al., 2019). The researchers used TPB to improve information security policy compliance by higher education institution employees. Hina et al. (2019) explained that the study's framework shows that the employees' intention to comply was motivated by the employee's attitude towards the understanding and availability of information security policies. Hina et al. (2019) also researched information security policy compliance, just like this study. However, in contrast to this research, the study of Hina et al. (2019) is a quantitative and survey research in a University in Malaysia and 301 participants.

Hina et al. (2019) opined that subjective norms show the expectations and processes of adopting security and compliance behaviors by the management, cybersecurity professional, and other employees (Hina et al., 2019). The researchers explained that subjective norms and self-efficacy are similar and equal, but they chose self-efficacy to study employees' protective behavior for their study. The researchers demonstrated that subjective norms directly impact employees' intentions to comply with

cybersecurity policies (Hina et al., 2019). Sommestad (2018) opined that based on results, TPB is the best framework for analyzing behavioral intention and that it is very straightforward.

Sommestad (2018) did a quantitative study on the relationship between work-related and information security policy compliance, using TPB as a framework. He applied a multilevel model to measure work-related groups' impact by utilizing a sample of questionnaires from 2,291 participants from 203 work locations, 119 companies, six sectors, and 38 professions (Sommestad, 2018). Sommestad (2018) applied shared features in work-related groups as factors of information security culture and concluded that work-related groups impact employees' information security behavior. The study of Sommestad (2018) was also on information security policy compliance, just like this research. However, in contrast to this research, Sommestad (2018) study is a quantitative and survey research conducted in Sweden and with 2,291 employees from different sites, firms and industries, and professions.

Kim and Kim (2017) studied the impact of compliance knowledge and support systems on the cybersecurity compliance behavior, using TPB and IT relatedness theory. After using TPB, the overarching framework revealed that compliance intention is affected by compliance intention belief and social pressure. Compliance behavior is affected by compliance knowledge in the active IT usage department and passive IT usage department (Kim & Kim, 2017). The study of Kim and Kim (2017) was also on information security compliance, just like this study. However, in contrast to this study,

the research is a quantitative and survey research in Seoul, South Korea, with 975 employees of S-OIL, an energy company in South Korea.

Jalali, Bruckes, Westmattelmann, and Schewe (2020) explored why hospital employees still click on phishing links using the TPB framework. The researchers collected data from 397 responses from 397 participants and, during the analysis of data, found out that the subjective norms, attitude, and perceived behavioral control (factors of TPB) and the trust (trust in Information security and collective trust) have a positive impact on compliance intention (Jalali et al., 2020). However, the authors also found out that compliance intention has no significant impact on compliance behavior. The employee's workload determines the number of times the employees will click on a phishing weblink (Jalali et al., 2020). The research of Jalali et al. (2020) was also on information security policy compliance, just like this study. However, in contrast to this study, the research of Jalali et al. (2020) uses a quantitative method and survey research. Likewise, unlike this study, it took place in three hospitals in the eastern region of the United States and on the web with 397 participants and three hospitals' networks.

Humaidi and Balakrishnan (2018), in their quantitative study on management support, users' compliance behavior, and information security policies, utilized TPB as the framework. The researchers collected data from 454 health workers in three clinics. The researchers made a cybersecurity policy compliance model from TPB, self-efficacy, management support constructs (from perceived behavioral control), and trust factors. The model was then applied to test the relationship between factors such as management support, self-efficacy, perceived trust, and user compliance behavior (Humaidi &

Balakrishnan, 2018). Humaidi and Balakrishnan (2018) opined that the findings revealed 52.8% of the variation in user compliance behavior; all determinants were significant. The management support had an indirect impact on user compliance behavior through perceived trust and self-efficacy among the research participants. Humaidi and Balakrishnan's (2018) research was also on information security policy compliance, just like this study. However, in contrast to this study, Humaidi and Balakrishnan (2018) research is a quantitative and survey research conducted in Malaysia with 454 health professionals and in 3 hospitals.

Transition and Summary

The purpose of my proposed study is to explore the strategies used by cybersecurity leaders to enforce cybersecurity policies. Section 1 comprises the introduction and foundation of my doctoral study. The section consists of the background, statement of the problem, statement of purpose, nature of the research, research question, and questions for the interview, conceptual framework, definitions, and significance of the research. Furthermore, Section 1 comprises a discussion of the assumptions, limitations, and delimitations of the study and concludes with a review of the academic and professional literature.

Section 2 comprises detailed explanations of the research methodology chosen for this doctoral study. The section outlines the researcher's role, analysis of the participants, analysis of the various research methods and design approaches, the types selected for this study, population sampling, ethical research, data collection, organization techniques, data analysis reliability, and validity. Section 3 will highlight an overview of the study,

the study's outcome, application to profession, social change implications, action recommendations, future research recommendations, reflections, and conclusion.

Section 2: The Project

The aim of the study was to research strategies that cybersecurity leaders utilize to enforce cybersecurity policies in an organization. Section 2 comprises the role of the researcher, participants, research methodology, research design, population and sampling, ethical research, data collection techniques and instruments, data organization and analysis, and reliability and validity.

Purpose Statement

The purpose of this qualitative study was to explore strategies used by cybersecurity leaders to enforce cybersecurity policies in an organization. The study population of the study was cybersecurity leaders—information system security officers, cybersecurity managers, and chief cybersecurity officers—associated with the enforcement of cybersecurity policies in three large organizations in southwest and northcentral Nigeria. The implication for positive social change lies in the strategies explored in this research leading to improved confidentiality of data, reduction in the occurrence of breaches, enhanced integrity of personal information, continuous availability of services, and the safety of life through improved cybersecurity compliance and awareness.

Role of the Researcher

The investigator is the primary data collection instrument (Marshall & Rossman, 2016). As the researcher, I was the primary instrument for data collection for this research. For this qualitative study, my role was to conduct interviews, collect data, analyze findings, and present the results. I aligned with Walden University's regulations

by avoiding plagiarism, ensuring accuracy in my work, and striving for credibility. Working with integrity and avoiding biases can be achieved by utilizing transparent and methodological research, such as using an interview protocol.

An interview protocol offers uniformity of interview questions for all participants and manages the researcher's precision and data saturation (Castillo-Montoya, 2016). Qualitative researchers use an interview protocol to ensure the research's consistency and dependability (Hoover, Strapp, Ito, Foster, & Roth, 2018). I asked all interviewees the same set of questions in the same way to ensure accuracy and reliability in the interviews and data that will be collected. The uniformity of the interview questions also aided me in identifying data saturation. In conjunction with interview best practices and creating a comfortable environment, I established a good rapport with each interviewee. Each question was open-ended and semistructured and written in a conversational format. The conversational format allows participants to feel more at ease and allows each participant to speak more freely (Ajodhia-Andrews, 2016).

I explored strategies for enforcing cybersecurity policies. I have 17 years of experience in IT and 12 years of experience in cybersecurity, which cuts across information security, cybersecurity, networking, datacentre management, project management, and general IT operations. I have worked in different IT roles in various organizations across several industry sectors, such as aviation, manufacturing, education, telecoms, IT, and an international organization. I have lived in Nigeria for over four decades and am familiar with the country's southwest and northcentral regions where the firms are situated. Ethical honesty and sincerity are essential in qualitative research

(Rolbiecki et al., 2017). I am currently an IT leader, and my personal experience in the topic is my rationale for engaging in the study. But I do not work for the companies I used as case studies; therefore, there was no personal predisposition and prejudice in the research. However, I still ensured that my knowledge and bias did not affect my findings. Bracketing is a method that researchers use to put aside their knowledge and experiences to gain knowledge from the participants' experiences (Sohn, Thomas, Greenberg, & Pollio, 2017). Therefore, I used bracketing during interviews and ensured I do not add my own bias to the study.

Ethical standards and protocols were also obeyed because the study involves human subjects. The noncompliance of a researcher to technical and ethical standards during data collection may lead to scrutiny (Vitak, Shilton, & Ashtorab, 2016). Therefore, it is crucial to follow the Belmont report's principles by aligning with ethical standards such as respect for human subjects, beneficence, nonmaleficence, and justice (Hammer, 2016; U.S. Department of Health and Human Services, 1979). These ethical standards and protocols include respecting participants by seeking their consent (Biros, 2018). It was also essential to follow the guidelines of the Institutional Review Board (IRB) of Walden University and get their approval before data collection. For this study, I followed the Belmont report standards and the guidelines of Walden University. Researchers are mandated to complete the protecting human research participants training offered by the National Institutes of Health Office of Extramural Research (Hammer, 2016). In line with the requirements, I have completed the training.

It is impossible to remove bias entirely; however, a researcher can reduce bias through interview protocols, data saturation, and member checking, using a personal lens throughout the study's data collection method (Fusch, Fusch, & Ness, 2017; Hoover et al., 2018). I was transparent with the interviewees, utilized an interview protocol for member checking, and used data saturation to reduce bias. I also viewed the data through a personal lens and reviewed the data to ensure accuracy. The protection of data subjects by de-identification is also a means of bias mitigation (Vitak et al., 2016), which I used to do unbiased scholarly research.

Participants

Participants in qualitative research should meet the eligibility criteria to ensure that the data collected satisfy the research objectives (Popescul & Jitaru, 2017; Roulston, 2018). The participants for this study were sampled on the criteria of experience and skill limited to participants involved with enforcing cybersecurity policies. The cybersecurity leaders included individuals who manage cybersecurity, information security, or network security and manage the cybersecurity policies and information security awareness training and programs for organizations. Other criteria I used for selecting participants included participants' experience in the enforcement or implementation of cybersecurity policies and participants' work and residence in southwest and northcentral Nigeria. Participants were selected based on their years of experience in enforcing or implementing cybersecurity policies.

Extensive screening of candidates can ensure that a multiple case study fits (Yin, 2016). To ensure participants satisfied the eligibility criteria, I contacted the gatekeepers

of three organizations operating within southwest and northcentral Nigeria by e-mail. A gatekeeper gives the researcher access to the participants (McFadyen & Rankin, 2016; Peticca-Harris, DeGama, & Elias, 2016). After applying for IRB approval for data collection from Walden University and receiving it, I sought participants who are cybersecurity leaders with the gatekeepers' assistance. Identifying the right participants, informing participants of the research objectives, and convincing them of the need for their participation are best practices of reaching participants (Maramwidze-Merrison, 2016). I identified potential participants from the list provided by the gatekeepers of the three firms. Then I sent letters of invitation and consent form to potential participants through the e-mail specifying the study's goals and details. I explained the study's purpose to the participants to obtain their consent to participate in the study.

Data were collected using open-ended questions during the interview sessions and reviews of the organization's document. Interviewers can establish working relationships with participants by building trust; however, the interviewer must refrain from influencing the interviewee (Yin, 2016). I developed a good working relationship with research participants involved by being transparent and trustworthy. Formal communication and the right interactions can promote transparency (Bamu, Schauwer, & Hove, 2016). My relationship with the participants was honest, respectful, and transparent.

Research Method and Design

Qualitative research and multiple case studies were the selected research method and design for exploring the strategies for enforcing cybersecurity policies. Qualitative

research entails developing holistic comprehension (Boddy, 2016). Accordingly, multiple case study research with several participants can be applied to develop a useful and high-level knowledge body (Boddy, 2016). A multiple case study was suitable to develop a detailed description of the strategies used by some organizations to enforce cybersecurity policies. The data collected from organizations via semistructured interviews and the examination of enterprise documents aided in understanding the strategies used by cybersecurity leaders in enforcing cybersecurity policies.

Research Method

A research study can be quantitative, qualitative, or mixed-method research. The qualitative method describes a phenomenon holistically, giving an in-depth explanation of motivations, attitudes, and behaviors (Abildgaard et al., 2016), which develops a detailed comprehension (Boddy, 2016). The qualitative method is beneficial for exploring the existence of a phenomenon (Yin, 2018) and enables researchers to understand and describe the participants' actions (Peck & Mummery, 2017). The qualitative study focuses more on why rather than on the phenomenon being studied and depends on participants' lived experiences to understand better the phenomenon (Christensen, Robinson, & Simons, 2016). Therefore, the qualitative research method was more suitable for this doctoral study because I explored the components of my research more deeply and contributed useful data to my study, which was about exploring the strategies for enforcing cybersecurity policies.

In contrast, quantitative research utilizes statistical testing and quantitative data analysis and generally uses probability sampling techniques to generalize data (Visser et

al., 2017). Quantitative researchers utilize experimental, quasi-experimental, and nonexperimental correlational design approaches to study cause-and-effect relationships among variables (King, Pullmann, Lyon, Dorsey, & Lewis, 2019). Researchers utilize quantitative research techniques to conduct numerical or mathematical measurements utilizing survey questionnaires. Quantitative research involves deductive and objective inquiry process to generalize statistical findings and test hypotheses (Boeren, 2018). With quantitative research, hypothesis testing and data analysis are done through statistical methods and experiments (Kasdan, 2016). The quantitative researchers utilize measurement or examination of relationships as the mechanism for data collection. Consequently, the quantitative research technique was not suitable for this research study because it did not require hypothesis tests, statistical tests, variables, numerical data, or the validity or reliability measures.

The mixed-method integrates qualitative and quantitative research methods to provide a fuller solution to problems (Gibson, 2017). The approach has the strengths of the two methods and reduces the weaknesses of the two techniques (Venkatesh, Thong, & Xu, 2016), integrating the two to a research instance (Venkatesh, Brown, & Sullivan, 2016). The mixed-method is more than merely combining qualitative and quantitative methods (Abdalla, Oliveira, Azevedo, & Gonzalez, 2018). Though the mixed method provides fuller and more significant data (Fusch et al., 2017), it costs more and takes more time. Overall, the mixed methods research offers a broader scope and better grasp of the subject matter to be studied compared to only one research method. However, given that my research study did not require quantitative or empirical data but rather a

qualitative semi and unstructured data, the mixed method was not appropriate for my research study.

Research Design

This qualitative research project employed a multiple case study approach. The multiple case study design approach was appropriate for this research to explore strategies for enforcing cybersecurity policies focusing on participants and organizations in southwest and northcentral Nigeria. The multiple case study design allows exploration of skills, knowledge, and strategies (Marshall & Rossman, 2016), which is suitable for capturing the rich quality, intensity, and variety of an inquiry from many perspectives (Civitillo, Juang, Badra, & Schachner, 2019). The multiple case study also allows for collecting data from documents, interviews, and observation (Yin, 2018). Thus, the design provides a better research reproduction prospect and more convincing results (Marshall & Rossman, 2016). The multiple case study approach is a practical approach to exploring strategies for enforcing cybersecurity policies. It is always better to use a case study to inquire about a phenomenon because it offers researchers various sources such as interviews, documents, or observations.

Some other design approaches may have been suitable. Even though the case study is the best approach, one potential approach was the phenomenological design approach. The phenomenological approach is a thorough inquiry into the participants' lived experiences (Bliss, 2016). In other words, the phenomenological design applies to studies on the viewpoints of participants about a particular occurrence, such as their individual experience about a phenomenon (Handwerker, 2018). Phenomenology

involves a viewpoint from which a researcher can explore the crux of experiences (Faronbi, Faronbi, Ayamolowo, & Olaogun, 2019). The phenomenological design might have fit if my study was to study the lived experiences of participants. However, my objective was to explore strategies for enforcing cybersecurity policies and not to study participants' lived experiences.

A second approach that could have been considered but was not applied is the ethnographic design approach. An ethnographic research approach involves studying social interactions by investigating shared patterns of beliefs, behaviors, and languages of participants in the same cultural group (Thornham & Cruz, 2018). A significant feature of ethnography is the research conducted on communities and groups seeking to observe language, culture, practices, or ideologies shared among such groups (Mol, Silva, Rocha, & Ishitani, 2017). The process of studying the cultural practices of respondents may extend the duration of the study. This research was not aimed to observe a group's culture but to explore the strategies cybersecurity leaders utilize to enforce cybersecurity policies.

Finally, a third approach I could have considered but did not utilize is the narrative approach. The narrative design verifies persons' stories as empirical knowledge (Bruce et al., 2016). The approach could be utilized to determine or define a group of persons' experiences and how the social, cultural, and physical environment influences and changes their practices (Haydon, Browne, & Van der Riet, 2018). A narrative approach stands on storytelling, and it hinges on how respondents see themselves and their experience of an occurrence or phenomenon (Kostov, Rees, Gormley, & Monrouxe,

2018). A narrative design is applied to form a comprehensive chronological story based on individuals' experiences (Beverland, Gemser, & Karpen, 2017). This study aimed not to tell a story but to explore the strategies cybersecurity leaders utilize to enforce cybersecurity policies.

Data saturation was also an essential part of the study. Every qualitative study needs to reach the point of data saturation where the collection of more data will not result in a piece of new information concerning the research question (Lowe, Norris, Farris, & Babbage, 2018). At the data saturation point, any further data becomes iterative, and no new theme is realized (Kline, 2017; Thomas & Briggs, 2016). Data saturation is achievable by employing member checking and data triangulation (Hagaman & Wutich, 2017). Therefore, to achieve data saturation within each organization and across them, I collected data from multiple sources, utilized member checking, and employed data triangulation within each organization. I did this by comparing the participants' responses from the semistructured interviews and extracting information from documents until no new theme came up.

Population and Sampling

Population

The study population was cybersecurity leaders associated with the enforcement of cybersecurity policies in three large organizations located in southwest and northcentral Nigeria. The cybersecurity leaders included information system security officers, cybersecurity managers, and chief cybersecurity officers. The study population is selected based on their level of knowledge and expertise concerning the overarching

research question (El-Masri, 2017; Malterud, Siersma, & Guassora, 2016). Therefore, the study population was eligible participants from each organization who have the experience and knowledge of enforcing cybersecurity policies in their organization.

The inclusion criteria included the participants who have been in the cybersecurity field of enforcing cybersecurity policies. With the gatekeepers' assistance, researchers get access to the participants (McFadyen & Rankin, 2016). I got access to participants through the gatekeepers to the organizations. I selected participants based on their skill and experience in enforcing strategies for enforcing cybersecurity policies. The study got limited to participants who are cybersecurity leaders involved in enforcing cybersecurity policies. The study population was all possible cybersecurity leaders from three firms. The selection of the population aligned with the purpose of the research. The selection focused on all cybersecurity leaders (in the three organizations) who have the experience and knowledge of the strategies for enforcing cybersecurity policies and have useful data for the study.

Sample Method and Justification

Purposive sampling is a non-random sampling method that supports the deliberate selection of the best-qualified participants (Etikan, Musa, & Alkassim, 2016). Sampling techniques in research are either probability (random) sampling methods or non-probability (non-random) sampling methods (Setia, 2016). Purposive sampling is a suitable method for selecting qualified participants when multiple case study cases are few (Etikan et al., 2016). This study required the most qualified participants, did not require a random sampling, and the cases were few (only 3). Therefore, I used purposive

sampling to select the best sample of the eligible participants to participate from the three large organizations, representing the three cases of the multiple case study.

The sampling involves collecting and analyzing the data until data saturation is achieved (Boddy, 2016; Van Rijnsoever, 2017). The sampling method I utilized is expert purposive sampling, which involved selecting four of the most qualified participants per organization for interview participation. According to Barratt, Ferris, and Lenton (2015), expert purposive sampling is selecting a sample of experts who are experts in collecting information in their fields of expertise. Selections made from expert purposive sampling are knowledgeable, skilled, and experienced in a particular study (Gentles, Charles, Ploeg, & McKibbon, 2015). The selected sample had the pedigree and knowledge of cybersecurity compliance and enforcing cybersecurity policies. In line with McFadyen and Rankin's (2016) expositions on gatekeepers and for data saturation, I utilized gatekeepers to get the names of four of the most qualified participants per organization. Also, I requested documents and data relating to organizational strategies, policies, risk management, security education, training and awareness programs, etc. that helped me assess and understand the strategies they utilize to enforce cybersecurity policies.

Sample Size and Justification

The sample size needed to achieve data saturation in a qualitative study should be selected based on appropriateness or requirements. The limit of the sample will depend on data saturation. Malterud et al. (2016) explained that the sample size needed to achieve data saturation depends on the population sample, the interview quality, the interview structure, and the participants' experience and knowledge of the phenomenon

under study. The appropriate sample size is imperative for planning and accountability (Tobin, Nugroho, & Lietz, 2016), and it depends on the requirements of the study. The sample size for this quantitative research was four participants per organization based on the research eligibility criteria.

The sample size was part of the data analysis, as I compared every information and identify the themes until I achieved data saturation across each firm. Boddy (2016) explained that the attainment of the data saturation occurs when there is no identification of a new theme after follow-up interviews. It is useful in the determination of sample size in a qualitative study.

Data Saturation

Researchers gather data and analyze data until attaining the data saturation point when any further data becomes iterative, and no new theme is realized (Kline, 2017; Thomas & Briggs, 2016). Hancock, Amankwaa, Revell, and Mueller (2016) explained that data saturation is the gold rating for qualitative research methodology. There will be no need to collect extra data from the participating organizations at the point of data saturation. Hagaman and Wutich (2017) explained that data saturation confirms the collection of enough data for a holistic analysis of data. Data saturation gives the qualitative researcher the green light to move to the next stage, the data interpretation stage. By interviewing four cybersecurity leaders per organization, getting data from them, and engaging them in member checking, I got all the interviewees' data based on the interview questions I asked them and achieved data saturation across the three participating organizations. I employed data triangulation within each participating

organization and across the three organizations (i.e., the 3 cases) by comparing the participants' interview responses and extracting data from documents until no new information came up to achieve data saturation.

Ethical Research

In this qualitative research, I ensured the ethical protection of the participants' data and privacy and ensured their informed consent respected their privacy and rights. Ethical protection is vital in any research that involves human subjects or participants**.** The informed consent form conveys the research objectives, data management, privacy, risk, gains, and participants' rights (Barnard, 2016). The main reason for consent in research involving human subjects is the protection and advancement of the participants' interest (Gelinas, Wertheimeir, & Miller, 2016). The participants have the right to decide if they want to participate or not (Forster & Borasky, 2018). Participants could decide to complete the consent forms before fixing and granting interviews (Santos et al., 2017).

IRB approval got obtained from Walden University before data collection began. The IRB approval number is 08-07-20-0495060. I began the data collection after the IRB approval. Before starting the data collection, in line with McFadyen and Rankin's (2016) recommendations, I contacted the gatekeepers in the organizations to be studied and sent consent forms through e-mail to the potential participants. The informed consent form document contains the information about the intended research, ethical concerns, existing risks, the participant's right to decline the request or withdraw from the research, the free will aspect of participation, and guidelines for the potential participant who wishes to participate.

Krajnović and Jocić (2017) explained that the informed consent form contains the participants' rights, information about the research, and guidelines on how to accept the request to participate. I gave a reasonable explanation about the research's objectives, the duration, procedures, gains, and risks in the consent form. Though researchers need to describe the research's objective to the participants, the participant's ethical protection from risks is much more necessary (Ross, Iguchi, & Panicker, 2018). The researcher owes the participants the ethical responsibility of protecting their data and privacy. It is vital to practice confidentiality because it helps create a trust relationship between the investigator and the participants. Ke (2016) explained that trust lessens the participants' concerns about the risks that could arise from the study.

In ethical research, the protection of participants is the top priority. I let the participants know they can voluntarily do their will. I informed them that they could withdraw from the research whenever they like through the letter of consent. Participants that withdraw will notify the researcher about their changed decision by e-mail. Participants withdraw for several reasons. The Belmont report's ethics provides all participants the privilege to withdraw from the research whenever they want to. I ensured compliance with ethical principles throughout the research by taking measures.

The participants' ethical protection includes non-disclosure of any personal information of the participants that may expose them or their organizations. I sought the consent of every participant. I did not deceive, intimidate, or force them against their free will. I respected their decision, even if they had decided to withdraw from the research for no reason. I followed the ethical guidelines of Walden University and the Belmont

report protocol to maintain high ethical standards, in line with Hammer's (2016) recommendations that it is essential to follow the Belmont report and follow the IRB's guidelines.

I informed participants that they would not get any monetary incentives or monetary benefits. Participants in this qualitative research did not receive any financial incentive or monetary compensation. Researchers may provide monetary benefits in some cases to entice the participants to participate in their study (Giles et al., 2016). Monetary incentives can affect or influence participants' behaviors in a qualitative study (Giles et al., 2016). In this case, I did not utilize financial incentives to entice any of the 12 participants to participate in this qualitative research.

Yin (2016) explained that interviewers build better relationships with participants by building trust. Therefore, I built a good rapport with the participants and explained that their participation is voluntary but that the information they provide will equip cybersecurity professionals and leaders with strategies for implementing cybersecurity policies in their respective organizations.

The researcher respected the privacy, rights, and integrity of participants and the firms studied. Singhal and Bhola (2017) explained that ensuring privacy entails protecting participants' identity in the research. To ensure ethical research, researchers must protect the participants' confidentiality and privacy (Singhal & Bhola, 2017). Therefore, I informed potential participants by e-mail that I will encrypt their identities with codes. I represented the participants with integers (e.g., Participant 1) and the firms with alphabets (e.g., Organization A). I encoded the participants' names, employers'

names, and job titles to protect their privacy and identity. Lancaster (2017) explained that the participants' anonymity is necessary throughout the study. Afterward, the interviewees could disclose some information that could cost them their jobs if the researcher exposes their identity.

Lancaster (2017) opined that protecting the participants' information with encryption is the best practice for privacy and confidentiality. I protected the document that has information about the participants and their companies with password protection. I kept the document and research study data in a lockable USB drive. I keep the soft copy of the research data another in another lockable USB drive and kept the hard copy documents in a locked cabinet in my apartment in line with the suggestions of Lancaster (2017). After five years, I will process the destruction of the research data according to the suggestion of Ferreira, Buttell, and Ferreira (2015) that the copies should be gotten rid of after five years. To destroy the study data, I will format the storage device that contains the documents from the three organizations and all the data from the interviews and member checking sessions and shred the hard copy documents.

Data Collection

This section discusses how data was collected and applied throughout the research. Semi-structured interviews with open-ended questions were the primary data collection method. The interview protocol guided data collection from the participants. The interview protocol captured details such as the background, demographics, and job position of the participant. The semi-structured interview was applied to develop a holistic picture of how cybersecurity leaders enforce cybersecurity policies.

Data Collection Instruments

I was the primary instrument for data collection, and I conducted semi-structured interviews utilizing open-ended questions during the qualitative multiple case study. Marshall and Rossman (2016) opined that the researcher is the primary instrument for data collection. The methods I utilized for collecting data are semi-structured interviews and a review of documents. I used a semi-structured interview with open-ended questions to draw out data from twelve interviewees. According to Boyaci and Güner (2018), semi-structured interviews allow participants to discuss their individual experiences.

Qualitative data get collected through in-depth semi-structured interviews, which provides a holistic understanding of the research question (Ridder, 2017). I utilized open-ended questions to allow the interviewees to discuss the answers holistically. With the application of semi-structured interviews, I explored the strategies that cybersecurity managers utilize to enforce cybersecurity policies.

Semi-structured interviews utilize open-ended questions so that the qualitative researcher can understand the participants' experiences and more detailed responses from them (Nebeker et al., 2016). Questions that are open-ended give participants a chance to expound their responses and assess the research question. I conducted semi-structured interviews with twelve participants, and each interviewee received open-ended interview questions and probing questions. I ensured I aligned with protocol in conducting the interview. I got the informed consent of the participants and reminded them before the interview. I interviewed the participants with the interview questions in Appendix B.

Dikko (2016) explained that an interview protocol is a set of rules and guidelines for conducting interviews. By enhancing interview protocols' reliability, qualitative researchers could improve the data collected from interviews (Castillo-Montoya, 2016).

The interviews occurred on the phone and through virtual communication. I recorded the interviews with the participants' consent and got them transcribed after the interview. I took notes during the interviews for the sake of data analysis. Qualitative research entails data collection from interviews, written notes, and recorded tapes (Renz, Carrington, & Badger, 2018). I gathered data by reviewing enterprise security policies, program manuals for education, training, awareness, access controls, internet, electronic mails, etc. I also collected data by reviewing organizational documents. The review process helped me analyze the contents and identify key themes, elements, and patterns that are significant in studying strategies for enforcing cybersecurity policies. The enterprise document review assisted in gaining knowledge about the cybersecurity and risk management policies, standards, and practices of the organizations studied.

After I completed the first interview, I conducted a follow-up interview for member checking. Researchers allow participants to do member checking to evaluate and validate their research findings (Iivari, 2018). Before the member checking, I listened to the interview recording, read the transcripts, and summarized the interviews into bulleted points. During the member checking, I discussed the bulleted summary in the follow-up interview with the participants. I allowed them to validate, clarify, or expound the interpretations to validate my understanding of what they had told me. I ensured the participants review the summary of findings and data interpretations from the previous

interview I had with them. I also ensured the participants clarify any unclear terminology in the previous interview that may affect the data analysis accuracy. Birt, Scott, Cavers, Campbell, and Walter (2016) explained that member checking allows participants to evaluate, correct, expound, and approve the correctness of the information they had shared during the interview. Member checking improves the integrity of findings, which is the foundation of the quality qualitative study, validates the findings, and aids in understanding the findings (Birt et al., 2016; Nelson, 2016). With the help of member checking, the participants can evaluate, edit and validate the accuracy of my knowledge and analysis of the participants' responses, thereby enhancing the reliability and validity of the research

Data Collection Technique

The data collection technique utilized by a qualitative multiple case study comprises interviews and reviews of documents to have a comprehensive knowledge of experiences or phenomena studied due to communication with the participants. The researcher is the principal instrument for collecting data (Clark & Vealé, 2018). I took note of assumptions that can hinder me from realizing objectivity in the research, being the principal instrument responsible for collecting data. In line with the recommendations of McFadyen and Rankin (2016), I sent out invitations to gatekeepers of the organizations requesting for participants who will participate in this research. After receiving the details of the participants, I sent out the consent form to the participants. The interviews occurred on the phone and through virtual communication in a secure environment.

It is essential to develop a good relationship with the participants and follow the interview protocol, according to Dikko (2016). Bamu et al. (2016) explained that formal communication and proper interactions yield transparency. Therefore there was transparency, formality, and order. For instance, every participant will answer the same number of questions. With the participants' consent, I timed and recorded the interview, according to the recommendation of Renz et al. (2018).

During the participants' response to the question, I took notes and recorded the interview with two recording devices in case of fail-safe backup in line with the recommendations of Renz et al. (2018). When the participants gave a short answer to some of the questions, they are meant to discuss in detail, and I asked them to elaborate. I also gave them room to discuss any extra information, solution, or recommendation. Rich content information is obtained through qualitative interviews because it allows interviewees to express themselves freely (Pipa & Sirbu, 2016). Zhang, Kuchinke, Woud, Velten, and Margraf (2017) explained that researchers could collect detailed information from participants through interviews. After the interviews, I reviewed the notes I had taken during the interview while the recorder recorded the participants' speech. The review helped me to understand the transcript of the interview better.

I asked the participants for a second interview to review the findings and confirmed the integrity of the findings and information disclosed during the initial interview. Iivari (2018) explained that the member checking method validates the findings of a qualitative study. Member checking is a standard method for improving the integrity of the findings of the research. Member checking allows the participants to

check and validate the accuracy of the data collected from them during the interviews (Nelson, 2016). Member checking happens when participants are asked by the researchers to evaluate the collected data for correctness and resonance (Bacon, Lam, Eppelheimer, Kasamatsu, & Nottingham, 2017). Birt et al. (2016) explained that researchers ask participants to do member checking to evaluate, edit, and explain the research findings. During the member checking, the participants could expound on the interview findings (Ntinda, Ntinda, & Mpofu, 2017). I conducted a follow-up interview for member checking. The participants were allowed to validate the data and clarify or expound any unclear thing they mentioned during the previous interview.

In line with the recommendations of McFadyen and Rankin (2016), I contacted the gatekeepers, and I reviewed with them the need for documents that will help me assess and understand the strategies the firms utilize to enforce cybersecurity policies. The discussion with the gatekeepers aided the process of collecting documents that served as secondary data. I informed the gatekeepers so that the participants knew the kind of documents I needed for review. I collected documents relating to organizational strategies, policies, risk management, security education, training and awareness programs, etc. The organizational documents enabled me to note the themes, patterns, and elements applied to the strategies the firms use to enforce cybersecurity policies. Collecting enterprise materials and strategies for enforcing cybersecurity policies helped me obtain extra more data.

Through the process of data triangulation, I gathered data from different sources and validated the research. Data triangulation involves gathering data from various

sources to obtain a more detailed understanding and confirmed research (Abdalla et al., 2018; El Hussein, Jakubec, & Osuji, 201). Conducting member checking and data triangulation in a study ensures the data correctness (Bacon et al., 2017). Doing the member checking and data triangulation leads to data saturation, which marks the end of data collection (Hagaman & Wutich, 2017; Nelson, 2016; Thomas & Briggs, 2016). I employed member checking and the process of data triangulation to ensure validity and data saturation.

Data Organization Techniques

The development, organization, protection, and storage of data improves access, management, and data regulation. Qualitative researchers utilize several data organization techniques like a coding dictionary, naming of files, or logs of research for the organization of data for easy tracking and control (Lasrado & Uzbeck, 2017). Reflective journals documents events and experiences that take place during interviews and reviews of the document. Cathro, O'Kane, and Gilbertson (2017) opined that researchers ought to organize their research logs, labels, themes, and notes for easier access. Reflective journals comprise opinions, personal views, sentiments, or feelings that could affect the research result.

I created secured folders and utilized unique file names. I also labeled and categorized documents concerning the respondents and institutions serving as case studies for easier access, in alignment with the best practices listed by Lasrado and Uzbeck (2017) and according to the recommendations of Cathro et al. (2017). I organized and encrypted documents, interviews, and member checking scripts. I organized the

documents in NVivo release 1.3 and will keep them in the cloud to ensure the safety of the data according to the recommendation of Lancaster (2017). Adetoro-Adewunmi and Damilola-Ajayi (2016) described NVivo as a qualitative data analysis computer software package that makes manual tasks easy, thereby enabling investigators to explore tendencies, discover themes, and make conclusions.

Organizational documents and notes, which are hard copies, are in a locked file cabinet in my apartment. I organized, categorized, and labeled documents for easier access, according to Cathro et al. (2017) recommendation. I kept a backup copy in a flash drive. I encoded the data for confidentiality according to the recommendations of Lancaster (2017). I will store all data (hard copy and electronic copies) for sixty months. I will delete soft copy documents (encoded copies, e-copies, and documents in the cloud) and destroy every hard copy document after five years, according to the recommendation of Ferreira et al. (2015) that suggests that the copies should be gotten rid of after five years.

Data Analysis

Researchers who engage in qualitative study ask open-ended questions to unravel the answers to the questions and get a deeper understanding of a phenomenon (Abildgaard et al., 2016). Hence the collection, organization, analysis, and interpretation of data are important in research. I utilized the interview protocol in Appendix B during data collection and then analyzed the data. Data compilation, disassembling the data, re-assembling the data, data interpretation, and data conclusion are the five data analysis stages (Yin, 2018). Data analysis gets improved with the aid of analytic procedures

(Kerwin-Boudreau & Butler-Kisber, 2016). I employed methodological triangulation for analyzing the data. Joslin and Muller (2016) opined that the main benefit of using this technique is that integrating several data sources will help the research scholar reduce the weaknesses in a data source.

The methodological triangulation is a suitable technique for data analysis to enhance research validity and an improved understanding of the research findings. I interpreted and analyzed the interview transcripts and reviewed the document in the multiple case study with the method. Methodological triangulation uses several data sources to improve the collection of detailed data to satisfy the research question (Abdalla et al., 2018).

The use of methodological triangulation for carrying out multiple case studies enhances data collection and analysis. The application of triangulation during multiple-case study research also enhances data and ensures that data is holistic (Abdalla et al., 2018**).** After interviewing the participants, I also collected organizational documents relating to cybersecurity policies, security education, training, and awareness documents from the participating organizations.

Data triangulation involves gathering data at varying periods from various sources to obtain a much more comprehensive explanation of the phenomena researched (Abdalla et al., 2018). Therefore, data triangulation analyzes many data sources for a research study to support research validation (El Hussein, Jakubec, & Osuji, 2016). The documents provided by the participants were reviewed, interpreted, and coded. Data triangulation takes place during the process of member checking to make sure of the

accuracy during the analysis of data (Bacon et al., 2017). Data triangulation ensures the authenticity of data (James, 2017). I used data triangulation to ensure the accuracy and authenticity of data.

The data analysis method consisted of identifying themes from the data collected. The qualitative data analysis ensures validity and reliability and possible descriptions from the findings (Yin, 2016). The data analysis concentrated on unraveling the central theme from the data collected. The analysis had to do with getting a holistic knowledge of the data to be collected. These included reviewing the interview transcript and member checking to have a comprehensive understanding of the data to be collected. I organized the data gotten from the interviews and documents using codes and subjects, respectively. I made a comparison of the different responses after transcribing the interview. I also managed themes and similarities, identified and analyzed concepts and patterns, and organized similar responses from participants into categories with the aid of NVivo release 1.3.

NVivo is computer software that researchers use to efficiently analyze qualitative data, thereby lessening their manual tasks and giving them more time to discover themes and outcomes (Atkins, Woods, Macklin, Paulus, & Atkins, 2016). Adewunmi, Koleoso, and Omirin (2016) applied NVivo to analyze transcripts of the interviews and the themes gotten from the research on benchmarking barriers among Nigerian facilities management. The analysis and organization of concepts and ideas designed for coding will identify significant themes, ideas, or patterns.

The thematic analysis aid the identification of pattern and themes across datasets while explaining the phenomenon under inquiry. The analysis of themes also has to do with familiarization with data, generation of initial codes, themes search and review definition and naming of themes, and report generation (Billen, Madrigal, Scior, Shaw, & Strydom, 2017; Wheeler & Mcelvaney, 2018). The thematic analysis method is appropriate for the analysis of qualitative data (El Said, 2017). I studied the information from the participants several times for familiarization, interpretation, and identification of themes. The process of coding will be done by labeling significant words, sentences, paragraphs, or sections. I used coding to produce themes for the analysis of data. Yin (2016) utilized techniques for examining data in qualitative studies, including those with multiple case study design approaches.

The technique of Yin (2016) involves analyzing data in different degrees, from common to specific ones. The interviews' analysis comprised the transcription of interviews and the conversion of the data into text format. I utilized a coding scheme for the data analysis. By combining significant codes, I generated general themes. The themes are specific and given names that offered a comprehensive understanding of the themes and the essence. I used axial coding by dividing interview transcripts into specific phrases, words, or paragraphs after the preliminary open coding. Mohajan (2018) described axial coding as analyzing significant categories, expanding, and connecting sub-categories. Mohajan (2018) also described open coding to label and identify essential words or phrases in an on-going process.

With the organizational documents, I used a similar process. I dissected the information into classes and subclasses, including recombining the data to reveal themes that seem to be alike. I used NVivo release 1.3 to analyze data from the interview transcript and organizational documents, using the coding methods to code and classify the data. Maher, Hadfield, Hutchings, and De Eyto (2018) explained that NVivo is applicable for analyzing content, word count, analysis of comparison, contexts, componential analysis, and taxonomic and domain analysis.

Reliability and Validity

Reliability and validity are imperative for every qualitative research study. Accurate data documentation is essential to make a qualitative study credible (Marshall & Rossman, 2016). Reliability is a repetitive process based on consistent research instruments with equal results (Posner, 2016). On the other hand, validity shows data accuracy (Spiers, Morse, Olson, Mayan, & Barrett, 2018). Validity examines if the researcher's outcome reflects the participant's thoughts, rather than questioning the credibility of the participants' responses to research questions (FitzPatrick, 2019). Wong-Riff et al. (2017) explained that validity develops data collection by analyzing the content. Korstjens and Moser (2018) explained that for a study to be considered trustworthy, reliable, and valid, researchers should consider the factors of dependability, credibility, transferability, and confirmability.

Qualitative researchers employ the processes of confirmability, dependability, transferability, and credibility to ensure the findings of the study are perfect and of high caliber (Korstjens & Moser, 2018). Therefore, I ensured my data's validity by employing

confirmability, dependability, transferability, and credibility to ensure my findings are complete.

Dependability

Dependability has to do with the consistency of research data over time (Forero et al., 2018). Qualitative researchers document their actions for dependability (Forero et al., 2018). Dependability defines the study's factors of consistency and reliability (Forero et al., 2018). Qualitative research is dependable if it is consistent with the same approach and yields the same findings and outcomes (Forero et al., 2018). Member checking, pilot testing, and review of transcripts enhance dependability. Research scholars must keep an audit trail or reflexive journal comprising full, holistic documents of the procedures and decisions that impacted the study (Korstjens & Moser, 2018).

The audit trail or reflexive journal portrays transparency as it allows a future research scholar to trail the path of a researcher's previous study. When the pattern generates the same findings, the research is dependable (Forero et al., 2018). Forero et al. (2018) opined that a dependable research study is reliable and valid.

To improve dependability, I transcribed the research findings and analyzed the data. I gave the participants the chance to examine my interview interpretation for additional recommendations to support the data. I also involved participants in member checking in checking the degree to which the study's findings are dependable. I employed member checking to validate the data from the main interview is accurate and dependable. Member checking enacts dependability in the research (Nowell, Norris, White, & Moules, 2017). Member checking ensures that the researcher's findings and

outcomes reflect the information that the participants gave to the researcher (Nowell et al., 2017). In other words, by utilizing member checking, researchers allow participants to evaluate and affirm the accuracy of the researcher's study findings.

The implementation of an audit trail or reflexive journal enhances the dependability of the study (Forero et al., 2018). In other words, by leaving behind an audit trail or reflexive journal in the form of a set of complete and holistic procedures on techniques, processes, and conversations with participants, future research scholars can trail that particular path to research with similar findings (Korstjens & Moser, 2018). I left an audit trail and reflexive journal by keeping documentation of the research and documentation procedures of all the phases of data collected from the interview and member checking, analyzed, and interpreted, done to enhance the research's dependability.

Credibility

Credibility is the trustworthiness and believability of the research findings (Nelson, 2016; Twining et al., 2017). In other words, credibility is the confirmation of the data (Bengtsson, 2016). Credibility is the degree of integrity and accuracy in recording the data (Marshall & Rossman, 2016). Credibility makes sure the findings of the research aligns with the objectives of the research. Credibility also signifies that the participants are the core agents in the research (Nelson, 2016). To enact credibility, researchers use the methodological triangulation of data to generate equivalent findings that are full and trustworthy. Accurate documentation is essential to the credibility of qualitative research.

I contrasted and compared participants' various responses to recognize the variances and similarities between themes, data sources, and links to the study.

Data triangulation and member checking are useful in ensuring the data's credibility and authenticity (James, 2017). I used data triangulation during the interviews and collection of documents obtained from the participating organization. While I also used member checking to make sure my research is credible. I also used methodological triangulation for the organization and analysis of the data. Triangulation is an essential aspect of a qualitative study. I applied triangulation to get supporting evidence from the data to be collected through interviews and the document review to ensure that the data collected from many sources satisfy the research question and draws a meaningful outcome. To ensure credibility, I documented the data precisely. Precise documentation is essential to the credibility of the study. I did not add my thoughts to the research findings.

Transferability

The transferability of research refers to how the study is transferable to another research (Forero et al., 2018). In other words, transferability implies a researcher's ability to act and transfer the findings to another context (El Hussein et al., 2016). Transferability involves getting dependable findings that are transferable to other contexts (Marshall & Rossman, 2016). Transferability is another critical factor of reliability in a qualitative study. Connelly (2016) opined that qualitative researchers could improve transferability by using quality content and precise explanations, locations, and open-minded and trustworthy participants.

I precisely documented observations, which included recorded assumptions. I also discussed the methods I used in the research study. I discussed participants' selection, interpretation of data, and how I reported findings. Having a comprehensive reflexive journal, a research method report can help other researchers decide transferable research findings and apply the findings for a future research study. An accurate report of the research will offer transferability to other researchers. Patino and Ferreira (2018) supported the possibility of transferability based on the knowledge that investigators offer sufficient data for other investigators to transfer findings.

Confirmability

Confirmability in qualitative research refers to the extent to which various reviewers could verify the interpretation of the research findings from a particular viewpoint (Morar et al., 2016). In other words, confirmability refers to the extent to which other researchers could verify the meaning of the research findings (Patino & Ferreira, 2018). For confirmability to be improved, there should be a review of themes by study group members (Morar et al., 2016). Confirmability also has to do with how the data is presented (Amankwaa, 2016; Bengtsson, 2016). The outcome should always reflect the participants' responses. I documented my observations throughout the research, thereby contributing to the confirmability of the data for presentation. To affirm the findings' accuracy and quality, I utilized triangulation to contrast and compare findings obtained from analyzing interviews and reviewing documents from the organizations.

Data Saturation

The process of data saturation enhances the caliber and content validity of a study. Without it, the caliber and validity of the study will be unconfirmed. Data saturation is reached in a qualitative study when the investigator has gathered sufficient data, and any additional data will not impact any change (Malterud et al., 2016; Tran, Porcher, Falissard, & Ravaud, 2016). At that point of data saturation, any further information becomes repetitive, as there is no discovery of a new theme (Kline, 2017; Thomas & Briggs, 2016). Data saturation is achievable by getting data from multiple sources (Hagaman & Wutich, 2017; Nelson, 2016). Therefore, to achieve data saturation, I employed data triangulation within each case (organization) and across the three organizations (i.e., the 3 cases) by comparing the participants' interview responses and extracting information from their documents until no information is collected. I also ensured data saturation by selecting participants through the process of purposive sampling and by member checking.

Transition and Summary

In Section 2, I further emphasized the purpose of my project by re-stating my purpose statement. I provided information on my project, indicating that my research aimed to explore the strategies used by cybersecurity leaders to enforce cybersecurity policies. I also discussed my role as the researcher and discussed the participants. I also discussed further on the research method and design approach of my proposed project. I employed a qualitative research method with three firms as multiple case studies, and I utilized purposive sampling to choose the participants I used to achieve data saturation.

The process of collecting data was in two phases. Data was collected using semi-structured interviews on the phone, and through virtual communication, from the review of documents provided by the companies. The data collected was analyzed and organized in NVivo release 1.3. I used methodological triangulation across the different sources of data to ensure data saturation. I analyzed the population and sampling for the study, and I analyzed the techniques of data collection, data organization, and data analysis for my research. I also did a description of my function as the primary data collection instrument. I also discussed ethical research, IRB requirements, and how I will follow the Belmont report's ethical guidelines while carrying out my research and avoiding bias. In this section, I also discussed how I would address reliability and validity with member checking. In Section 3, I progressed and finished the research by presenting an overview of my study, the research outcome, the application to practice, social change implications, action recommendations, future research recommendations, reflections, and research conclusion.

Section 3: Application to Professional Practice and Implications for Change

Grounded in TPB, this qualitative case study explored the strategies cybersecurity leaders utilize to enforce cybersecurity policies. Section 3 comprises an overview of my study, the research outcome, the application to practice, social change implications, action recommendations, future research recommendations, reflections, and research conclusion.

Overview of Study

The purpose of this qualitative multiple case study was to explore strategies used by cybersecurity leaders to enforce cybersecurity policies in an organization. The data came from semistructured interviews via phone and virtual conversations conducted with 12 research participants based in southwest and northcentral Nigeria. There were 20 documents collected and analyzed on organizations' cybersecurity strategies and policies, risk management strategies, security education, training, and awareness programs provided by the study participants or referred by them. All participants had experience working on enforcing cybersecurity policies. I utilized member checking and data triangulation to increase the validity of the findings from the research. The results comprise four major themes—security awareness and training, communications, technology control, and management support—which characterize the strategies that cybersecurity leaders use to enforce cybersecurity policies in organizations.

Presentation of the Findings

The overarching research question of this study was, "What strategies do cybersecurity leaders use to enforce cybersecurity security policies in an organization?"

As a result of data collected from the three participating organizations through interviews with 12 participants from the three cases and reviewing the 20 documents provided by the participants, four main themes emerged. The themes are security awareness and training, communication, technology control, and management support. The participants' names and participating organizations were encrypted. For quick identification and understanding, the encrypted PyCz code was used to identify the participants and participating organizations. The letter P stands for the participant. The letter C stands for the participating company, and *y* and *z* are the integers indicating the interview's order. References in the tables also represent each theme's frequency of occurrence, and the count represents the number of documents and participants supporting each theme.

Theme 1: Security Awareness and Training

Security awareness and training emerged as the first theme from the case study of the three organizations. This theme indicates that before enforcing a cybersecurity policy in an organization, security awareness and training must be in place. Employees must be educated and trained on their security responsibilities and must be made aware of security risks. In every organization with cybersecurity policies, security awareness and training programs play a critical role in implementing the policies. Without security awareness, cybersecurity leaders may not be able to enforce cybersecurity policies effectively. Cybersecurity leaders use security awareness and training programs as an effective strategy to implement and implement cybersecurity policies.

The results from the interviews and member checking of participants supported the security awareness and training theme. All 12 participants from the three participating

organizations asserted that they utilize security awareness and training to enforce cybersecurity policies in their respective organizations (see Table 3). P1C1 explained that his organization uses security awareness and training to get their employees trained and security-aware to comply with their organizational cybersecurity policies. P1C1 stated that, as cybersecurity leaders, they train and educate their employees on their organizational cybersecurity policies, the existing security risks, recent security breaches, current industry cybersecurity trends, and their security responsibilities in ensuring the security of their organization's cyberspace.

Table 3

Frequency of First Major Theme

	Participants		Documents	
Major theme references	Count	References	Count	References
Security awareness and training	12	197	16	51

Participants noted the ranking of security awareness as a strategy for enforcing cybersecurity. P2C1 explained that security awareness and training strategy is the best strategy for enforcing cybersecurity policies. P4C2 noted that security awareness and training comes first before any other strategy. P3C1, P4C1, P1C2, P3C2 agreed that the security awareness and training strategy is the best strategy among all the strategies for enforcing cybersecurity policies. However, the other seven participants rate security awareness and training strategy as an effective strategy on the same scale as the remaining three strategies for implementing cybersecurity policies.

Most participants stated the importance of security training. P3C1 noted that security awareness and training strategy sensitizes their employees on the cybersecurity policies, what the security policies say, and why they should follow the security policies. P1C2 also explained that their security awareness and training sensitize their employees on the cybersecurity policies and educate them on the proper and acceptable cybersecurity attitude and culture they should exhibit regarding organizational data, assets, and resources. P1C3 explained that if employees do not know why they instructed them to follow specific cybersecurity guidelines, they will not understand why they need to comply with the cybersecurity policies. P4C1 further explained that security awareness makes the employees aware of why the cybersecurity policies are in place and aids the employees know the purpose of the cybersecurity policy and understand the security benefits of having the cybersecurity policy in place and their security obligation to implement the cybersecurity policy.

The participants shared their methods for training employees on cybersecurity. P1C1 said that his organization utilizes induction programs, continuous e-learning, and e-mail awareness to educate their employees on cybersecurity, security risks, and cybersecurity policies. P2C1's organization utilizes induction training programs organized by their human resources, e-mail awareness, and phishing campaigns to educate their employees on their cybersecurity policies and the need for cybersecurity compliance. P1C2's organization uses classroom-based training, instructional programs, webinars, and Zoom meetings for security awareness and training, as well as educational materials and videos. P2C3's organization conducts security awareness and training using

online computer-based training courses. Similarly, P3C3's organization uses weekly SMS and e-mail alerts for awareness, does quarterly computer-based security awareness training programs, and has an information security week once every year. In the same vein, P4C3's organization does cybersecurity courses and use online training sites to train their employees. P2C1 also noted that his cybersecurity team had tailored security awareness and training to suit their organization's various roles:

> For instance, somebody sends a mail to you. If you are not sure of it, delete it. If a suspicious sender sends you a mail with an attachment or link, don't click on the attachment or the link. delete the message. Or If you come work and see a flash drive on your system, find out why it is there if you did not plug it.

All 12 participants also noted that their organization uses assessment as part of their security awareness and training strategy to measure their employees' cybersecurity policy compliance while enforcing cybersecurity policies. P4C1 noted that their employer does security awareness tests as part of their security awareness training and education. P1C1 stated that "We review our employees' cybersecurity policy compliance through the security awareness tests and assessments we conduct during our quarterly security awareness programs." Similarly, P2C1 explained that his organization conducts security awareness assessments for the employees to ensure that they are adhering to the cybersecurity policies and examine how serious they have taken security awareness training. Both P1C1 and P2C1 attested that security awareness assessments are used by organizations to review employee cybersecurity compliance. P2C1 further explained that they sometimes create and send out simulated phishing e-mails to everybody to test their

cybersecurity compliance level and their familiarity with their industry's current cybersecurity trends. P3C1 also stated, "from time to time, we send out simulated phishing e-mails to all staff to examine their level of cybersecurity policy compliance and knowledge of cybersecurity risks." P3C1 explained that their security awareness assessments are brief and concise so that their employees do not spend too much time taking the tests. P1C1 and P2C1 said that their cybersecurity team reviews their employees' cybersecurity compliance through security awareness programs every quarter of a year; P1C2, P2C2, and P3C2's organization reviews its employee cybersecurity compliance every 2 years; and P2C3, P3C3, and P4C3's organization reviews its employee cybersecurity compliance every year.

Documents from the participating organizations also support the security awareness and training theme. Out of the 20 documents reviewed, 16 of them validated the security awareness and training theme, enhancing the theme's reliability and validity. The 16 documents include documents from the three participating organizations on security awareness, risk management, cybersecurity policies, and risk-based cybersecurity framework. The documents on cybersecurity policies reveal the security awareness procedures, security responsibilities of the employees, security responsibilities of the organizations' cybersecurity leaders, and the security awareness and training programs. The security awareness documents contain detailed information and guidelines on data privacy and security tips for the organizations' employees and stakeholders. The document on risk management provided details on the organization's awareness objective, awareness benefits, and awareness impact. The document on risk-based

cybersecurity framework provides details on cybersecurity awareness control as a cybersecurity resilience strategy, guidelines on cybersecurity awareness training, and cybersecurity awareness as a continuous security monitoring strategy. The documents show comprehensive details on the security awareness and training theme and support the participants' responses.

Current scholarly literature also supports the security awareness and training theme as a best practice. For example, research has shown that awareness of cybersecurity policies yields employee cybersecurity compliance by changing employees' attitudes and behaviors to prevent security risks (Belanger et al., 2017; Cong et al., 2017; Torten et al., 2018; Yazdanmehr & Wang, 2016). Training employees on cybersecurity aids the management of cyber threats (Bartnes et al., 2016; Miranda, 2018), as cybersecurity awareness and cybersecurity policy awareness significantly impacts employees' attitudes toward compliance (Bauer & Bernroider, 2017; Park et al., 2017a). Bauer et al. (2017) recommended that organizations customize security awareness and training programs based on their employees' skill level and area of responsibility. Therefore, security awareness and training is an important part of organizations' cybersecurity policies and should frequently occur to improve security awareness (Gerhold et al., 2017; Mamonov & Benbunan-Fich, 2018; Safa et al., 2016).

Further, research has indicated that cybersecurity security awareness strategy is a best practice utilized to safeguard sensitive data. Hatfield (2018) demonstrated that security awareness reduces the occurrence of social engineering attacks. Similarly, Ki-Aries and Faily (2017) explained that insufficient security awareness and lack of right

employee attitude and behavior lead to a higher risk of security breaches. Manworren et al. (2016) explained that security awareness and training positively affect employees' cybersecurity policy compliance and reduce organizations' security incidents. Security awareness and training programs are needed to train, educate, and enable employees to understand cybersecurity policies (Flowerday & Tuyikeze, 2016).

The security awareness and training theme also directly aligns with the conceptual framework of the study, the TPB. The TPB framework supports the security awareness and training theme because security awareness aligns with the attitude-toward-behavior construct of TPB. For example, Belanger et al. (2017) used the TPB framework and discovered that security awareness positively impacts attitude toward behavior in their study. The theme is also consistent with Dang-Pham et al.'s (2017) research grounded in the TPB framework on the reason why employees share information security knowledge and found out that employees having a better attitude towards security behavior, influenced by security awareness, tend to share security advice with others. The security awareness theme is also consistent with the results of Bauer and Bernroider (2017), who applied the attitude toward behavior construct of the TPB in their study on cybersecurity compliance in a large European banking organization and found out that security awareness influences the attitudes toward behavioral compliance of the employees. In summary, the attitude-toward-behavior construct of TPB encourages security awareness and training.

The interviews, member checking, and document review triangulation validated the importance of security awareness and training. The current and existing literature also

further validated the security awareness and training theme, as it aligns with the literature. Lastly, the TPB framework also supports and encourages the use of security awareness and training.

Theme 2: Communication

Communication emerged as the second theme from this case study of three organizations. This theme shows that a communication strategy must be in place for cybersecurity policies to be enforced in an organization. Communication is essential to get the buy-in of management and employees at all levels. Cybersecurity leaders must communicate cybersecurity policies, security risks, and security updates to their management, and management must communicate with employees before cybersecurity compliance. The cybersecurity leaders ensure that employees have read, understood, and agreed to abide by the policy. If there is no communication, the management and employees cannot understand the cybersecurity policies, not to mention align with it. Hence, communication is crucial for the enforcement of cybersecurity policies in an organization.

The findings from the interviews and member checking of participants supported the communication theme. All three organizations' participants asserted that communication is one method they utilize to enforce cybersecurity policies (see Table 4). P1C1 explained that the management communicates the security risks, policies, and updates to the employees through its human resources department. P1C1 said that his cybersecurity team also communicates to all staff what their organizational cybersecurity policies are all about, the existing security risks, and their security responsibilities in

ensuring their organization's security. P1C1 also mentioned that his organizations have a CISO who develops cybersecurity policies and communicates them to executive management. P3C1 noted that communication strategy enhances the employees' understanding of the cybersecurity policies and why they need to comply. P4C1 explained that the purpose of cybersecurity policy and its benefits are communicated to the employees to understand the cybersecurity policies and comply with them. P1C1, P2C1, P3C1, and P4C1 agreed that communication is one method their organization uses to enforce cybersecurity policies.

Table 4

Frequency of Second Major Theme

	Participants		Document	
Major theme reference	Count	References	Count	References
Communication	12	64	17	52

Participants offered different ways that cybersecurity is communicated with employees. P1CI explained that broadcasting the cybersecurity policy updates, risks, and awareness is done continually through e-mail. P1CI explained that when his cybersecurity team observes a cybersecurity risk happening in the industry, they send risk updates through e-mail to their employees. P1CI also mentioned that they also communicate every change in cybersecurity policy to their employees. P1C1, P2C1, P3C1, P4C1 agreed that their organization uses communication via e-mail to enforce cybersecurity policies. In the same vein, P1C2, P2C2, P3C2, and P4C2 agreed that their organization communicates to its employees via e-mail, web portal, and virtual

communication. Similarly, P1C3, P2C3, P3C3, P4C3 agreed that their organization communicates to its employees through SMS and e-mail.

Documents from the participating organizations also support the communication theme. Out of the twenty documents reviewed, seventeen of them validated the communication theme, as seen in Table 4, and were used to achieve triangulation, enhancing the communication theme's reliability and validity. The seventeen documents include documents from the three participating organizations on cybersecurity policies, communication strategies, and communication on cybersecurity tips. The documents on communications on cybersecurity tips reveal detailed security tips for the organization's employees and stakeholders.

The documents on cybersecurity policies highlighted communication strategies and security information on the safekeeping of assets, acceptable use of e-mail messaging, disposal of information, data encryption, monitoring, data protection, backup restore and archives, antivirus policy, control against mobile and malicious codes, electronic channels, personal handheld devices, and official mobile devices. The documents show comprehensive details on the communication theme and support the responses of the participants.

Current scholarly literature also supports the communication theme as a best practice. Niemimaa and Niemimaa (2017) explained that companies communicate their cybersecurity policies and the consequences of non-compliance to their employees. Curran (2015) also demonstrated that broadcasting the policies and the penalties to employees are part of the strategies organizations utilize to enforce cybersecurity

policies. Dhillon et al. (2016) explained that security values and goals communicated can lay the foundation of cybersecurity compliance and culture.

Ki-Aries and Faily (2017) suggested that communicating cybersecurity policies in innovative ways can enhance cybersecurity policy compliance. Da Veiga and Martins (2017) also listed cybersecurity culture communication as one of the best practice strategies for implementing cybersecurity policies. Flowerday and Tuyikeze (2016) also opined that organizations utilize the communication of security notices, newsletters, and posters to employees to stimulate cybersecurity policy awareness and compliance. Torten et al. (2018) also supported the evidence of communication of acceptable cybersecurity practices to ensure that employees are cybersecurity-compliant, fully aware, and educated on security risks, to avoid compromising confidentiality and integrity, and availability of data in organizations.

Cybersecurity leaders communicate the management's organizational cybersecurity expectations to their employees. The cybersecurity executive communicates and gets the word out to their employees. The cybersecurity managers tailor the communication towards security risks from daily activities rather than just the likelihood of occurrences, thereby imparting more understanding and awareness of security risks (Pham, Pham, Brennan, & Richardson, 2017). Cybersecurity executives have the responsibility of helping the employees to understand their cybersecurity policies. The cybersecurity leaders' approach is to make the cybersecurity policies succinct, clear, consistent, and meaningful and to describe behaviors and attitudes that are acceptable or unacceptable regarding cybersecurity (Pham et al., 2017).

Cybersecurity leaders develop down-to-earth security reference materials for communicating security knowledge to their employees. The cybersecurity leaders should also update the security guidelines in their employee handbook. While communicating to employees, the cybersecurity chiefs ensure that their cybersecurity presentations and campaigns are down-to-earth, friendly, and applicable to a real-life scenario to win them. In other words, in enforcing the cybersecurity policies, the cybersecurity executives ensure they don't only communicate compliance but also make the cybersecurity policy enforcement process enjoyable, satisfying, and attractive to the employees (Pham et al., 2017).

Corporate cybersecurity chiefs implement incident response programs for communication of incidents response. Cybersecurity leaders acknowledge and communicate security breaches. Cybersecurity leaders update security policies and communicate them to their employees through e-mails, memos, and posters. Similarly, cybersecurity executives apply strategies such as having cybersecurity workshops for the communication of security education. In the same vein, Cybersecurity leaders also utilize cybersecurity help desk for communication and quick resolution of cybersecurity incidents (Pham et al., 2017).

Communication directly aligns with the conceptual framework of the study, the TPB framework. Communication aligns with the attitude toward the behavior construct of TPB. In other words, the TPB framework supports the communication theme because communication aligns with the 'attitude towards behavior' construct of TPB. A favorable attitude towards cybersecurity policies gives a corresponding good intention to comply

with cybersecurity policies (Menard et al., 2017). In theory, communications influence employees' behavioral intentions (Belanger et al., 2017). Belanger et al. (2017) used the TPB in their research on information security policy compliance and found out that communication positively impacts employees' attitudes towards policy compliance.

Belanger et al. (2017) opined that communication affects employees' attitudes towards policy compliance in their study, grounded in the TPB framework. They used survey questionnaires to measure the relationship between communication and attitude towards cybersecurity behavior. Pham et al. (2017) also examined the TPB framework in their study on information security and people in which they interviewed 23 participants from personal contacts, Facebook, and LinkedIn, and discussed how communication influences compliance intention and actual cybersecurity policy compliance.

The triangulation of the interviews, member checking, and document review validated the importance of communication. The current and existing literature also further validated the communication theme, as it aligned with the literature. Lastly and finally, the TPB framework also supports and encourages the use of communication.

Theme 3: Technology Control

Technology control emerged as the third theme from the case study of the three organizations. The emergence of the technology control theme indicates that its role in the implementation of cybersecurity policies in organizations. Cybersecurity executives emphasize that using people and process strategies to enforce cybersecurity policies is not enough; technology must be applied. In implementing cybersecurity policies, cybersecurity leaders utilize technology to monitor, check, and execute cybersecurity

compliance. Organizations employ security information and event management, security event and incident management, firewalls, antivirus, intrusion detection system, access controls, intrusion prevention system, vulnerability assessment, penetration testing, data loss prevention software, and many other technical monitoring, audit, and compliance check tools to implement cybersecurity policies.

The results from the interviews and member checking of participants supported the technology control theme. All three organizations' participants mentioned that their organizations employ technological monitoring, auditing, and compliance tools to monitor, check, and enforce cybersecurity compliance (see Table 5). P1C1 explained that his organization uses technology to secure their data, infrastructure, user access, remote access, etc. P2C2 also noted that their organization uses technology tools such as firewalls, the antivirus system, all the devices network access control to enforce cybersecurity policies.

Table 5

Frequency of Third Major Theme

	Participants		Document	
Major theme references	Count	References	Count	References
Technology	12	188	16	85

P1C1 also explained that his organization uses the technology tools and solutions to ensure that they are on top of security threats, mitigate threats, and be aware of their cyber risks. P1C1 noted that his organization uses technology tools like a web application firewall to enforce its cybersecurity policies that prevent user access to prohibited websites. P1CI explained that his cybersecurity team has technical solutions that prohibit

unauthorized user access to data and restrict unwanted mails like phishing e-mails. P1C2 also noted that their organization use firewall and monitoring tools to enforce compliance.

Automated monitoring systems are often used by organizations to monitor their employees' activities (Flowerday & Tuyikeze, 2016). P2C1 also explained that their organization utilizes technology to enforce cybersecurity policies using technologies that monitor and check user access, remote access, and user privileges. P2C1 explained that his cybersecurity team utilizes access monitoring tools to monitor access. P2C1 noted that his cybersecurity team uses technology to manage privilege access, collect logs for reviews, and check their employees' cybersecurity compliance. P2C1 cited an example of network segmentation that his cybersecurity team uses to restrict user access and privileges. P2C1 stated that "Only authorized users with rights and authorization can access some servers and data." P2C1 also explained that his cybersecurity team utilizes data loss prevention solutions to monitor user access and prevent data loss.

P3C1 also discussed their organizations use technology to restrict phishing mails. P3C1 also explained how her organization uses firewall technology for threat analysis and for monitoring their employees. P3C1 opined that their organization uses technology such as an identity service engine for authentication of employees. P3C1 also mentioned that his cybersecurity team uses security posturing technology that prevents employees from accessing their network if their system is not secured but accepts them after their system is secure with the latest patches. P4C1 also explained that their organization uses technology for monitoring, auditing, compliance checking, and cybersecurity compliance

enforcement. P4C1 explained how their organization uses technology to monitor the security posture of their network. P4C1 also explained how his cybersecurity team uses technology to monitor all the activities on their database servers to ensure no unauthorized activity.

P4C1 also explained how their organization uses technology, such as an integrity monitoring solution that monitors changes or modifications on the servers' file systems. P4C1 also explained using technology tools such as security information and event management software to monitor their network and collect log reports. P4C1 also explained that their organization uses a technical network tool that scans every activity in their internal system with complete visibility. P4C1 explained that technology is utilized to prevent cyber-attacks from attacking their organization, thereby helping them stay protected and cybersecurity policy compliant.

Another technology tool that organizations utilize in enforcing cybersecurity policies is data loss prevention software. All twelve participants explained that data loss prevention software is a technology tool they utilize to enforce cybersecurity compliance. P1C1 explained that his organization utilizes a data loss prevention tool to mitigate security threats. P3C2 also explained that his organization employs a data loss prevention tool to check the security risk of e-mails before they send them. Data loss prevention prevents the cyber exploitation of data and hardens the cybersecurity of organizations. P3C3 and P4C3 agreed that their organization uses data loss prevention to curb against data leakage in ensuring that its employees don't release confidential information.

P2C3 noted how technology plays a role in enforcing cybersecurity policies, using an example of password policies. P2C3 explained that some configurations get done at the network level and application before password policies get implemented. P2C3 discussed the value of technology while explaining that if people and processes are taken care of, and technology is left out, the cybersecurity policy implementation process will fail.

P4C2 noted that his cybersecurity teams use technological tools such as firewalls access controls, patching programs, antivirus systems, two-factor authentication, monitoring tools, detective control, and preventive control to enforce cybersecurity policies. Similarly, P3C3 opined that his cybersecurity team utilizes technology such as firewalls, antivirus, endpoint detection and response systems, security evident, and event monitoring systems to enforce cybersecurity policies. P3C3 explained that his cybersecurity team uses the monitoring technology tool for auditing and logging and ensures that employees are aware that they monitor and track their activities.

P4C3 explained that his cybersecurity team uses endpoint detection and response, cisco devices, checkpoint, and other different technologies. P3C3 noted that his organization uses technology to implement cybersecurity policies by implementing automated and technology controls such as endpoint detection and response, data loss prevention, firewall, database activity monitoring, technical security tests, and checks. Also, P3C3 noted that his cybersecurity team sets technical security and hardening baselines, conducts penetration testing and vulnerability assessment, configuration assessments, sets group policies to manage endpoints and privileges of users, and writing

programs for risk mitigation. P3C3 noted that their organization protects itself against security risks, threats, vulnerabilities, exploits, and technology strategy breaches.

P3C3 illustrated how his cybersecurity team enforces cybersecurity compliance by changing an employee's privileges through the process of changing the group policies of the employee's official system on the active directory. P3C3 noted that his cybersecurity team also enforce cybersecurity policies and track cybersecurity compliance with the use of technology by using agents on servers and systems. Furthermore, P3C3 noted the agents include trend micro endpoint detection and response tools with intrusion prevention system roles. P3C3 explained that with the trend micro, his cybersecurity team could manage the host's firewall and control everything on the system. P3C3 explains that this technology tool can uncover the ciphers, algorithms, and protocols on the computer system the noncompliant and unauthorized employee uses.

Documents from the participating organizations also support the technology control theme. Out of the twenty documents reviewed, sixteen of them validated the technology control theme, as seen in Table 5, and were used to attain triangulation, enhancing the technology control theme's reliability and validity. The sixteen documents include documents from the three participating organizations on information security policies, risk management, risk-based cybersecurity framework, and technical tips. The documents on technical tips reveal technical tips that employees and stakeholders of the organization should use to achieve cybersecurity compliance and protect themselves from security risks and breaches. The document on the risk-based cybersecurity framework

revealed technical controls, information security management systems, and network threat prevention technology such as intrusion prevention systems.

The document on the information security policies highlighted technology requirements such as technical controls, monitoring, regular testing of information system technical control compliance by using tools to detect network intrusion, the performance of penetration testing, validation of the functional design, and implementation of the system technical controls, the performance of technical compliance checking as part of the system change management process and vulnerability assessment, and independent assessments and reviews to assess information system compliance to security policy. The documents show comprehensive details on the technology control theme and support the responses of the participants.

Current scholarly literature also supports the technology control theme as best practice. Safa et al. (2016) also explained that an acceptable security strategy must include technology and be comprehensive. In other words, Safa et al. (2016) noted that technology is a best practice that must be part of every cybersecurity strategy used in organizations. Flowerday and Tuyikeze (2016) conducted a study on what, how, and who of information security policy development and implementation and explained that best practice technology tools such as automated monitoring systems as best practices play a role in implementing cybersecurity policies in organizations.

Choi (2016) conducted a study on information security managers' role in the effectiveness of information systems security and demonstrated that cybersecurity leaders implement cybersecurity policies using best practice technology strategies such as

surveillance and monitoring employees' activities to detect violations and violators. Similarly, Hwang and Cha (2018) researched potential threats to employees' information security compliance. They explained that organizations utilize best-practice technology tools such as network firewalls, document encryption technology, network monitoring technology, and device control technology strategies in enforcing cybersecurity policies.

Technology directly aligns with the conceptual framework of the study, which is the TPB framework. The technology control theme aligns with the perceived behavior control construct of TPB. In other words, the TPB framework supports the technology control theme because technology aligns with the 'perceived behavioral control' construct of TPB. Cuganesan, Steele, and Hart (2018) examined the TPB framework in their study of the relationship between top management, norms, and information security behavioral control and attitudes, noting that that behavioral intention and actual compliance behavior is predictable by perceived behavior control and explained that technology tools such as monitoring systems positively impact perceived behavioral control.

Jalali et al. (2020) utilized the TPB framework in their research on employee compliance using phishing links in hospitals and noted that technology usage affects employees' compliance intention. Jalali et al. (2020) noted that technology usage positively impacts compliance intention in their study, grounded in the TPB framework. They used 397 questionnaires from 397 participants to examine the relationship between TPB factors, technology, and compliance intention. The researchers also noted that TPB factors impact employees' cybersecurity policy compliance intentions (Jalali et al., 2020).

Flowerday and Tuyikeze (2016) also examined the TPB framework in their study on developing and implementing information security policies, rating TPB as a useful framework for research on employees' behavioral intention cybersecurity policy compliance. Flowerday and Tuyikeze (2016) noted that TPB explained that a person's compliance intention is impacted by the 'perceived behavioral control' construct and noted that using technology tools like an automated monitoring system is useful in enforcing cybersecurity policies.

The triangulation of the interviews, member checking, and document review validated the importance of technology. The current and existing literature also further validated the technology control theme as best practice, as it aligned with the literature. Lastly and finally, the TPB framework also supports and encourages the use of technology.

All this evidence, including the study results, indicates that technology is an effective strategy for enforcing cybersecurity policies and that technology positively impacts employee cybersecurity compliance. Employees who fully grasp technology's purpose in enforcing cybersecurity policy policies accept its usage by being careful with what they do in cyberspace.

Theme 4: Management Support

Management support emerged as the fourth theme from the case study of the three organizations. This theme indicates that there must be management support for cybersecurity policies to be enforced in an organization. The top management of an organization has to be involved in the enforcement of cybersecurity policies for the

process to be successful. Most often, employees don't comply with cybersecurity policies, except there is an order from the top. Hence, the top-down management approach plays a crucial role in the enforcement of cybersecurity policies. The executive management of organizations approves a cybersecurity compliance audit, reviews the audit report, provide resources for technology and cybersecurity implementation, and uses sanctions to bring their employees to comply with the cybersecurity policies.

The findings from the interviews and member checking of participants supported the management support theme. All three organizations' participants asserted that management support is one method they utilize to enforce cybersecurity policies (see Table 6). All the participants explained that their management uses sanction to enforce cybersecurity compliance. P1C1 explained that their management uses sanctions to punish employees who breach their cybersecurity policies to compel them to comply. Similarly, P1C2 explained that when their employees fail to comply with the cybersecurity policies, they get sanctioned by their organization's executive management to compel them to abide by the policies. P1C3 explained that employees who are aware of the cybersecurity policies but do not adhere to them get sanctioned.

Table 6

Frequency of Fourth Major Theme

	Participants		Document	
Major theme references	Count	References	Count	References
Management support	12	137	10	60

P3C1 explained that their organization sanctions employees who fall victim to simulated phishing e-mails they send to their e-mail account to assess their cybersecurity compliance. P3C1 and P4C1 explained that sanction is one of their management methods to enforce cybersecurity compliance. The eight participants in the other two organizations also mentioned sanction by their management in enforcing cybersecurity policies. P1C3, P2C3, P3C3, and P4C3 explained that management uses sanctions for enforcing cybersecurity policies and approves disciplinary action when an employee fails to comply with cybersecurity policies. However, P2C1, P2C2, and P3C2 explained that although management uses sanction to enforce cybersecurity policies, a sanction is the least effective method of enforcing cybersecurity policies imparts fear in the hearts of the employees.

Another way executive management supports cybersecurity compliance is by appointing a C-level staff with the job title of CISO who will oversee cybersecurity and be reporting to them on issues related to cybersecurity. All the twelve participants mentioned that their organization has someone playing the role of a CISO and that it is a management's strategy to enforce cybersecurity policies. P1C3 explained that management appoints a role for cybersecurity and that management is ultimately accountable for cybersecurity in the organization. P1C1 explained that his organization's CISO oversees every aspect of its cybersecurity and regularly communicates its cybersecurity resilience posture to its executive management. P1C3 explained that the CISO must brief the board and make them aware of what is going on and the need for cybersecurity to secure the environment.

Management support also comes in the form of funds and support. P1C1 explained that the management supports cybersecurity by releasing funds to purchase technology tools utilized for cybersecurity compliance. P4C3 stated, “Without the financial backup of management and their buy-in, we can not procure anything.” P1C2 explained that his cybersecurity team enjoys top management support while continually improving their organization’s cybersecurity posture.

P3C2 explained that before any change management occurs, management approval is required. P4C2 explained that cybersecurity leaders get support from management in the form of directives to enforce cybersecurity policies. P1C3 noted that management support is crucial in approving cybersecurity. Also, P1C3 noted that before any cybersecurity project can be feasible, the executive management must understand the project’s need before they can buy-in and be committed to it.

P1C3 noted that executive management is committed to cybersecurity policy enforcement and that the enforcement of cybersecurity policy is a core commitment of the management. P1C3 explained that his organization’s top management is committed to enhancing cybersecurity by approving the budget and release of cybersecurity implementation funds. P2C3 noted that cybersecurity is a priority of the board. Similarly, P1C3 explained that his organization’s management reviews cybersecurity implementation to see the present situation and plan for action and improvement. P1C3 stated that “Management is ultimately accountable for cybersecurity in the organization.” Eight participants from the three participating organizations explained that their

companies are regulated, and it is a major reason why their board and management take cybersecurity compliance as a top priority.

Documents from the participating organizations also support the management support theme. Out of the twenty documents reviewed, ten of them validated the management support theme, as seen in Table 6, and were used to achieve triangulation, enhancing the management support theme's reliability and validity. The ten documents include documents from the three participating organizations on cybersecurity policy, risk-based cybersecurity framework, risk management, and management support. The documents on management support revealed how management supports cybersecurity compliance. The document on risk management highlighted how management supports cybersecurity compliance and details on management review of security risks, cybersecurity governance, and the role of top management in risk management and cybersecurity.

The document on cybersecurity policy highlighted top management's commitment to enforcing cybersecurity compliance, the role of executive management in cybersecurity, and the function of management in ensuring the suitability of the cybersecurity policies for organizational purpose, improving the effectiveness of cybersecurity, communicating the policy, and reviewing it for continued suitability. Similarly, the risk-based cybersecurity framework document contains details on cybersecurity governance and oversight, the board of directors' responsibility toward cybersecurity, the responsibilities of top management, and the responsibility of the CISO.

The documents show comprehensive details on the management support theme and support the participants' responses from the three participating organizations.

Current scholarly literature also supports the management support theme as best practice. Ki-Aries and Faily (2017) explained that management support is a critical determinant in implementing cybersecurity compliance. Rothrock et al. (2018) explained that executive management should oversee cybersecurity policy. Ifinedo (2016) also explained that organizational cybersecurity policies could be more effective with its executive management support.

Flowerday and Tuyikeze (2016) explained that without management support, the enforcement of cybersecurity policies will not be worthwhile. Top management's support makes the cybersecurity policy implementation possible (Alreemy et al., 2016) because management provides the project's funds and resources (Steinbart et al., 2016). Niblett (2016) explained that management support is one of the factors that determine compliance. Niblett (2016) also explained that organizations utilize punishment to enforce compliance. Similarly, Pham et al. (2016) also explained that organizations utilize sanctions to ensure cybersecurity policy compliance.

The executive management is involved in the entire process of cybersecurity policy implementation (Flowerday & Tuyikeze, 2016). Management is involved in budgeting and funding of cybersecurity, and without the approval of top management for the release of funding for cybersecurity and the implementation of cybersecurity policies, the project goal can not be achievable (Flowerday & Tuyikeze, 2016). In recent times, most large organizations have a c-level management position, the CISO, that oversees

cybersecurity. The presence of a CISO makes cybersecurity policy compliance easier to implement. Cybersecurity leaders use management support as an effective strategy to enforce and implement cybersecurity policies.

Management support directly aligns with the conceptual framework of the study, the TPB framework. The management support theme aligns with the TPB framework's perceived behavior control construct (Humaidi & Balakrishnan, 2018). In other words, the TPB framework supports the management support theme because management support aligns with the 'perceived behavioral control' construct of the TPB framework. Humaidi and Balakrishnan (2018) utilized TPB in their research on the effect of management support on information security policy compliance in hospitals and discovered that user compliance behavior is impacted by management support.

Humaidi and Balakrishnan (2018) discovered that management support has a positive impact on perceived behavioral control in their study, grounded in the TPB framework. They used questionnaires from 454 participants to examine the relationship between management support and user compliance behavior. Humaidi and Balakrishnan (2018) noted that management support significantly changes user cybersecurity behavior. Similarly, Flowerday and Tuyikeze (2016) also examined the TPB framework in their research on the development and implementation of information security policies noting that management support was the second most essential strategy for enforcing cybersecurity policies through top-down direction and intentions of management.

Cuganesan et al. (2018) also examined the TPB framework in their research of the relationship between top management and the three TPB factors, norms, and

information security behavioral control and attitudes, noting that that behavioral intention and actual compliance behavior is predictable by perceived behavior control, and explained that senior management support had a significant impact on the attitude towards cybersecurity behavior and subjective norms of the employees of their organization.

The triangulation of the findings from interviews, member checking, and document review validated the importance of management support. The current and existing literature also further validated the management support theme as best practice, as it aligned with the literature. Lastly and finally, the TPB framework also supports and encourages the use of management support. All evidence indicates that management support positively impacts employee cybersecurity compliance and is an excellent strategy for enforcing cybersecurity policies.

The four findings, precisely security awareness and training, communication, technology control, and management support, are all indispensable components of how cybersecurity leaders enforce and implement cybersecurity policies in organizations. Each finding, on its own, plays a crucial function in the cybersecurity policy enforcement process. However, when combined, they form a comprehensive combination that makes cybersecurity policy implementation possible and makes employee cybersecurity policy compliance successful. Effective enterprise cybersecurity governance in an organization requires active cybersecurity policies. Therefore utilizing these rich combinations of proven, tested, and practical strategies for implementing cybersecurity policies is essential for organizations.

Applications to Professional Practice

The specific IT problem investigated in this study was that some cybersecurity leaders lack strategies to enforce cybersecurity policies in an organization. Many firms do not have capable strategies for enforcing cybersecurity policies. However, the organization that participated in this research incorporated strategies towards cybersecurity policy implementation and compliance. The three participating organizations operate in heavily monitored industry sectors; therefore, the participants' details showed that the need for cybersecurity compliance with the industry regulations enhances cybersecurity policy enforcement.

The study's strategies showed the importance of security awareness and training, communication, technology, and management support in implementing cybersecurity policies and enforcing cybersecurity compliance. Cybersecurity leaders in different sectors of the economy may use this research's findings as a guide in enforcing cybersecurity policies within their organizations. The participating organizations' strategies in implementing cybersecurity policy implementation aligned with the constructs of TPB.

Similarly, the strategies align with the TPB framework's constructs, and the employees in the participating organizations demonstrated positive subjective norms, positive attitude to behavior, and positive perceived behavioral control in complying with their organizational cybersecurity policies. By applying the TPB constructs to cybersecurity policy compliance, cybersecurity leaders in organizations across various

sectors could better understand their employees' human behavior and have effective cybersecurity compliance strategies that promote desired employee behaviors.

Subjective Norms

The subjective norm is positively impacted by management support, as evident from the study. Cuganesan et al. (2018) noted that management support positively impacted norms toward cybersecurity compliance. In other words, management support influences the norms of employees towards cybersecurity compliance. Based on the results of the study, cybersecurity leaders can utilize management support to enforce cybersecurity policies. The subjective norms, being a predictor of intention and cybersecurity compliance, predicts cybersecurity policy enforcement (Yazdanmehr & Wang, 2016). All the participants mentioned that management support is a significant factor in the enforcement of cybersecurity compliance.

Based on this study's result, it is evident that aligning organizational cybersecurity policies with global information security standards like ISO 27000 series and best practices enhance world-class security culture and improves cybersecurity compliance. Organizations align with risk-based cybersecurity guidelines by having a board oversight and responsibility, cybersecurity budget, a CISO, an Information security steering committee, independent internal audit, risk management system, and cybersecurity resilience assessment. Organizations also align with best practices by having cybersecurity self-assessment, cybersecurity operational resilience using an up-to-date inventory of authorized software and cyber threat intelligence, metrics, monitoring and reporting for compliance, and having a cyber incidence report.

The study's documents show that the risk-based cybersecurity framework enhances organizational security processes, policies, and programs. An effective risk management system with a risk assessment and risk management strategy mitigates cybersecurity risks and breaches effectively. The participants confirmed that risk management is a critical aspect of cybersecurity policies. The participating organizations comply with industry regulations by aligning with the risk-based cybersecurity framework and guidelines and updating their cybersecurity policies and security programs such as security awareness and training.

Subjective norms determine intention and behavior towards cybersecurity policy compliance. Hence, subjective norms relate to an organizational cybersecurity culture. Management support has a significant impact on the subjective norms of their employees. Organizations address the subjective norms with support from their top management and through enforcement of cybersecurity policies.

Attitude Toward Behavior

Attitude towards behavior is positively influenced by security awareness and training strategy and management support, as evident from this study's results. Belanger et al. (2017) noted that security awareness and training positively affects attitude toward behavior. Similarly, Cuganesan et al. (2018) explained that management support significantly impacts management support. This study's result also indicates that security awareness and management support positively impact employees' behavior. Employees of organizations develop cybersecurity culture through security awareness and training programs and with the support from management. All the participants in the research

mentioned security awareness and training and management support during the interview sessions.

The participants explained how they utilize security awareness and training programs and management support strategy to enforce the cybersecurity policies. The participants also explained how they ensure that employees attend their security awareness programs before accessing their information systems. Security awareness and training make the employees see the need to comply with the cybersecurity policies and enlighten them on their security responsibilities. The security awareness programs were structured to meet the employees' educational needs and security needs.

The security training and awareness expose the security risks of non-compliance with the employees' security policies and educate them on what to do to mitigate the risks and prevent security breaches. The security awareness programs mitigate security risks associated with social engineering and phishing. Consequently, the security programs transform the weak human links, which once fell prey to security risks to strong human firewalls. Similarly, cybersecurity awareness makes the employees knowledgeable and aware of security risks and protects them against such risks. The security training and awareness communicates the updates in the cybersecurity process, programs, or policies.

A practical security awareness and training program focuses on the employees' attitudes and behaviors to prevent security breaches and mitigate security risks. The security awareness and training enlighten the employees on the magnitude of security vulnerabilities that could occur when there is a lack of cybersecurity policy compliance.

The security awareness programs also help build mature cybersecurity and risk culture. When organizations have successfully incorporated security awareness and training programs, they have successfully addressed the attitude towards their employees' cybersecurity behavior.

Perceived Behavioral Control

Perceived behavioral control is influenced by technology and management support, as evident from the study. Cuganesan et al. (2018) explained that technology positively impacts perceived behavioral control. Similarly, Humaidi and Balakrishnan (2018) noted that management support significantly influences perceived behavioral control. All the research participants mentioned management support and technology during the interview session and explained how the two strategies influence cybersecurity policy compliance. Support from executive management enhances the development and sustenance of a risk and cybersecurity culture within the organization and leads to the cybersecurity policies' enforcement.

The fear of executive management is often the beginning of employee compliance. With management support, security controls get implemented and automated, and employees comply with security measures such as guidelines, procedures, and policies. The top-down approach from top management to employee enforces compliance and enhances security culture. With management support, employees can know the acceptable cybersecurity behavior and comply with cybersecurity policies, thereby developing a cybersecurity culture. The involvement and support of executive

management make perceived behavioral control towards cybersecurity compliance much better.

The perceived behavioral control also becomes better with technology. In other words, technology improves perceived employee behavior towards cybersecurity policy compliance. Cuganesan et al. (2018) also noted that technological monitoring and evaluation impact perceived behavioral control. Similarly, Jalali et al. (2020) explained that technology positively impacts compliance intention. These indicate that technology is useful in enforcing cybersecurity policies. When employees understand the use of technology in enforcing cybersecurity policy compliance, they accept it, comply with the policies, and are careful with what they do online.

The findings from the research show the strategies which the participating companies use to enforce cybersecurity policies. The research made use of the TPB framework as a lens. This research may assist cybersecurity leaders by offering them strategies for enforcing cybersecurity policies, enabling them to overcome the challenges that come with the process, and enabling them to understand the phenomenon of cybersecurity better to create and implement better policies.

The research study may contribute to cybersecurity by the exploration of the strategies for enforcing cybersecurity policies. These findings may also enhance organizational cybersecurity programs and also enhance the organizational cybersecurity culture of organizations. The study's findings may also support cybersecurity policy implementation across various industries and sectors of the economy.

Implications for Social Change

The implications for positive social change of this research lies in the potential that this study's findings may have a significant positive impact on the public in the field of cybersecurity. Security breaches usually have a significant influence on society because of the loss of data and financial losses. By utilizing the findings in this study, cybersecurity leaders can implement cybersecurity measures that could enhance the public's confidence by assuring them of the safety of their personal information, the confidentiality of their data, integrity of their data, and the availability of their services.

This study's findings may also benefit the public by providing information regarding how they can enhance their security habits and awareness, prevent data theft, avoid identity theft, and mitigate privacy breaches. They may also avoid being victims of social engineering and hacking and avoid inconvenience due to security attacks and unauthorized access to their personal information. Thus, this research findings may reduce the occurrence of security risks and breaches and enhance the public's confidence by assuring them of the protection and privacy of their data, information, assets, and resources.

This study's findings may also contribute to the existing cybersecurity body of knowledge by providing information on cybersecurity policy compliance and cybersecurity policy implementation. Similarly, the findings from this study could be a great resource to schools, centers of learning, and current and future bachelors, masters, doctoral, and post-doctoral degree students who may take an interest in learning about

cybersecurity policy compliance to develop or improve their knowledge, skills, and abilities or to do research in the field.

This study's findings may also benefit private and public organizations and institutions in various sectors of the economy and countries by providing proven international best-practice cybersecurity strategies. The findings from this study could also help promising cybersecurity leaders who wish to enforce cybersecurity policies in their respective organizations and require a detailed understanding of the challenges of implementing cybersecurity policies and how to handle such issues. This study's findings could also benefit several organizations that wish to enforce and implement cybersecurity policies to improve their security culture, reduce their security risks, and protect their respective organizations' assets, data, infrastructures, and resources.

Recommendations for Action

Cybersecurity leaders who don't have the experience and knowledge of what it takes to enforce cybersecurity can use this study's results to implement and enforce their cybersecurity policies, improve employee compliance, and mitigate the occurrence of security risks and breaches. Cybersecurity policy compliance is an essential aspect of the security programs of the organization. Cybersecurity leaders can integrate the findings of this study into the security programs of their organizations.

Cybersecurity executives should strive to understand their employees' human behavior better and also strive to develop a positive organizational cybersecurity culture that promotes cybersecurity policy compliance and positive employee behavior and attitude towards their cybersecurity policies. Cybersecurity policies should be designed

so that employee cybersecurity compliance will not be a difficult task. In a way, employees will see cybersecurity compliance as part of their responsibility.

Furthermore, cybersecurity leaders should make cybersecurity training and awareness programs a critical aspect of their organizational cybersecurity policies. The cybersecurity leaders should partner with the human resource department to conduct psychometric tests to understand the employees' different personality behavioral traits and provide appropriate training for each category's employees.

Every large organization should have a c-level role whose focus will be on cybersecurity management. Also, executive management should support cybersecurity by approving the security programs of their cybersecurity leaders. Without the moral and financial support of the management, cybersecurity policy implementation and compliance will be impossible. Employees will find it very difficult to comply with cybersecurity policies and embrace a risk and cybersecurity culture without the top management's strong hand and back up. The management's financial support is also compulsory for the consistent maintenance and upgrade of their security infrastructure, the execution of security programs, staff training, and enforcement of cybersecurity policies.

Cybersecurity leaders should endeavor to conduct yearly security audits and review and update their organizational cybersecurity policies to align with global best practices and to be able to tackle current security risks and threats. The cybersecurity executives should also endeavor to have a communication strategy for the communication of security policy updates, security expectations, guidelines, procedures,

standards, threat intelligence, information on security risks and breaches, training and awareness plans and incident response, etc. to staff and stakeholders in compliance to cybersecurity best practices and regulations. The communication strategy should also include collaboration and sharing of security knowledge and strategies.

I shall disseminate this study through different means. After I receive CAO approval, the study would be published by Walden University scholar works and by ProQuest. I will disseminate my findings through e-mail to all the twelve participants who actively participated in this study. I will add a copy of the study to the list of my publications on ResearchGate, Google Scholar, ORCiD, and Academic.edu. Also, I intend to cite the study in journal articles I will publish later. These proposed actions will further extend the global impact and dissemination of the study.

Recommendations for Further Study

There are quite a few recommendations for further study. One recommendation is that future researchers could conduct the study with more participants and partner organizations. This recommendation relates to this study's limitation of small sample size and delimitation of three organizations mentioned in section one. Although the sample size was small, this study gained a lot from having cybersecurity leaders provide comprehensive and in-depth information that aligns with up to date literature. Albeit, there is a possibility that including more participants and more participating partners may reveal other areas of interest that are not in this study and could contribute further to the current research.

A second recommendation is for future researchers to research further in every geopolitical zone of Nigeria or another country. This recommendation relates to one of the delimiters mentioned in section one of this study. Although the participating organizations from the southwest and northcentral regions were only three, this study benefited immensely from the organizations and their cybersecurity leaders who provided detailed information that aligns with current research. Albeit, there is a possibility that including more geopolitical zones or conducting the study in another country may reveal other areas of interest that were not revealed in this study and could contribute further to the current literature.

The third recommendation is that further research could use a quantitative research methodology and anonymous survey design to mitigate bias from the participants. Although all participants were masked by the researcher who assumed that the participants gave the right answers and information, this recommendation would further encourage future participants to disclose information and mitigate their risks of withholding information due to fear of losing their jobs.

Another recommendation is that a future researcher could use another conceptual framework to extend the research. This recommendation will allow future researchers to utilize another lens or see the problem from another perspective. Future researchers could also consider using other cybersecurity-related theories, rationality-based behavior theories, or criminology related theories such as GDT, PMT, SCT, RCT, TRA, or Institution theory as a framework for further studies. These would allow the researcher(s) to use other constructs not used in this study and examine other behaviors not captured.

Reflections

My experience during the doctoral study is a vivid example of the fact that diligence, resilience, consistency, and patience breeds success. I never did research that is so thorough and time-consuming as the DIT study. I stayed awake several nights and remained focused throughout the process. I maintained constant communication with my chair and was flexible and very open to corrections and guidance from my chair and committee members. I was also very patient with gatekeepers and participants. My experience as a DIT student shows that success can be sure with hard work, resilience, and a never say die attitude. I never gave up, despite my numerous challenges and commitments during my program.

I had always had a flair for research from my undergraduate days of my first bachelor's degree when my professors and a Nobel prize nominee recognized my research ability. However, I never conducted any study of this magnitude. After passing through it all, I feel very fulfilled that I continued and finished my DIT journey. During this journey, I have learned about conceptual frameworks, social change, and how to be a scholar-practitioner. I have also learned a lot about qualitative research and developed expert-level research skills and advanced level IT skills that have contributed to my career.

My doctoral study, "strategies for enforcing cybersecurity policies," aligns with my aspirations as a cybersecurity professional. I have learned a lot from the research, and I believe many professionals will also learn from it. I experienced delay while waiting for letters of cooperation from the second and third participating organizations, which was a

criterion for IRB approval. But now I can smile because it is all over. I would like to say diligence, consistency, resilience, and patience win the race to all those coming behind. If I can make it, then they can make it.

Conclusion

Cybersecurity leaders enforce cybersecurity policies in their organizations to prevent security breaches and to enforce cybersecurity compliance. Enforcing cybersecurity policy compliance requires time and effort because a lot of time is needed to develop a security culture. Cybersecurity policy compliance also requires management support. The executive leadership must buy into the cybersecurity policy implementation and support it with funds, approval, and communication to all members. The participating cybersecurity leaders implemented cybersecurity policies in this study's participating organizations because of the support they got from their management. Strategies such as security awareness and training build a security culture and enforce cybersecurity policies. These strategies reduce risk and mitigate security breaches. This study can educate cybersecurity professionals and leaders on implementing or enforcement of cybersecurity policies using management support, security awareness and training, communication, and technology control strategies.

References

Abdalla, M. M., Oliveira, L. G. L., Azevedo, C. E. F., & Gonzalez, R. K. (2018). Quality in qualitative organizational research: Types of triangulation as a methodological alternative. *Administração: Ensino e Pesquisa, 19*(1), 66-98. doi:10.13058/raep.2018.v19n1.578.

Abildgaard, J. S., Saksvik, P. O., & Nielsen, K. (2016). How to measure the intervention process? An assessment of qualitative and quantitative approaches to data collection in the process evaluation of organizational interventions. *Frontiers in Psychology, 7,* 1-10. doi:10.3389/fpsyg.2016.01380.

Adetoro-Adewunmi, Y., & Damilola-Ajayi, O. (2016). Attitudes of Nigerian facilities management professionals to the benefits of benchmarking. *Facilities, 34*(7), 468-492. doi:10.1108/f-06-2014-0057.

Adewunmi, Y. A., Koleoso, H., & Omirin, M. (2016). A qualitative investigation of benchmarking barriers in Nigeria. *Benchmarking: An International Journal, 23*(7), 1677-1696. doi:10.1108/BIJ-06-2014-0055.

Adhikari, K., & Panda, R. K. (2018). Users' information privacy concerns and privacy protection behaviors in social networks. *Journal of Global Marketing, 31,* 96-110. doi:10.1080/08911762.2017.1412552.

Adjerid, I., Peer, E., & Aquisiti, A. (2018). Beyond the privacy paradox: Objective versus relative risk in privacy decision making. *MIS Quarterly, 42*(2), 465-488. doi:10.25300/MISQ/2018/14316

Ajodhia-Andrews, A. (2016). Reflexively conducting research with ethnically diverse

children with disabilities. *The Qualitative Report, 21*(2), 252-287. Retrieved from https://nsuworks.nova.edu/tqr//

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

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211. doi:10.1016/0749-5978(91)90020-T

Ajzen, I. (2011). Behavioral interventions: Design and evaluation guided by the theory of planned behavior. In M. M. Mark, S. I. Donaldson, & B. Campbell (Eds.), *Social psychology for program and policy evaluation* (pp. 74-100). New York, NY: Guilford.

Ajzen, I. (2014). 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*(2), 131-137. doi:10.1080/17437199.2014.883474

Ajzen, I., & Albarracin, D. (2007). Predicting and changing behavior: A reasoned action approach. In I. Ajzen, D. Albarrazin, & R. Hornik (Eds.), *Prediction and change of health behaviour: Applying the reasoned action approach*, 3-18, Mahwah, NJ: Erlbaum.

Almeida, F., Carvalho, I., & Cruz, F. (2018). Structure and challenges of a security policy on small and medium enterprises. *KSII Transactions on Internet & Information Systems, 12*(2), 747-763. doi:10.3837/tiis.2018.02.012

Alreemy, Z., Chang, V., Walters, R., & Wills, G. (2016). Critical success factors (CSFs)

for information technology governance (ITG). *International Journal of Information Management, 36*(6), 907-916. doi:10.1016/j.ijinfomgt.2016.05.017

Amankwa, E., Loock, M., & Kritzinger, E. (2018). Establishing information security policy compliance culture in organizations. *Information & Computer Security*, 26(4), 420-436. doi:10.1108/ICS-09-2017-0063

Amankwaa, L. (2016). Creating protocols for trustworthiness in qualitative research. *Journal of Cultural Diversity, 23,* 121-127. Retrieved from https://www.questia.com/library/p587/journal-of-cultural-diversity

Andrews-Speed, P. (2016). Applying institutional theory to the low-carbon energy transition. *Energy Research & Social Science, 13,* 216-225. doi:10.1016/j.erss.2015.12.011

Angst, C. M., Block, E. S., D'Arcy, J., & Kelley, K. (2017). When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches. *MIS Quarterly, 41*(3), 893-916. doi:10.25300/MISQ/2017/41.3.10.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior, 69,* 437-443. doi:10.1016/j.chb.2016.12.040.

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.2016.02.065

Armitage, C. J., & Conner, M. (2001). Efficacy of the theory of planned behaviour: A

meta-analytic review. *British Journal of Social Psychology, 40*(4), 471-499. doi:10.1348/014466601164939

Arpaci, I., & Baloglu, M. (2016). The impact of cultural collectivism on knowledge sharing among information technology majoring undergraduates. *Computers in Human Behavior, 56*, 65-71. doi:10.1016/j.chb.2015.11.031

Atkins, D., Woods, M., Macklin, R., Paulus, T., & Atkins, D. P. (2016). Advancing qualitative research using qualitative data analysis software (QDAS)? Reviewing potential versus practice in published studies using ATLAS.ti and NVivo, 1994-2013. *Social Science Computer Review, 34*(5), 597-617. doi:10.1177/0894439315596311

Aurigemma, A., & Mattson, T. (2017a). Deterrence and punishment experience impacts on ISP compliance attitudes. *Information and Computer Security*, *25*(4), 421-436. doi:10.1108/ICS-11-2016-0089

Aurigemma, S., & Mattson, T. (2017b). Exploring the effect of uncertainty avoidance on taking voluntary protective security actions. *Computers & Security, 73*, 219-234. doi:10.1016/j.cose.2017.11.001

Auxilia, M., & Raja, K. (2016). Ontology centric access control mechanism for enabling data protection in the cloud. *Indian Journal of Science and Technology, 9*(23), 1-7. doi:10.17485/ijst/2016/v9i23/95148

Ayyagari, R., & Figueroa, N. (2017). Is seeing believing? training users on information security: Evidence from java applets. *Journal of Information Systems Education, 28*(2), 115-122. Retrieved from http://jise.org/l

Bacon, C. W., Lam, K. C., Eppelheimer, B. L., Kasamatsu, T. M., & Nottingham, S. L. (2017). Athletic trainers' perceptions of and barriers to patient care documentation: A report from the athletic training practice-based research network. *Journal of Athletic Training*, *52*(7), 667-675. doi:10.4085/1062-6050-52.3.15

Balozian, P., & Leidner, D. (2017). Review of IS security policy compliance: Toward the building blocks of an IS security theory. *The DATA BASE for Advances in Information Systems, 48*(3), 12-43. doi:10.1145/3130515.3130518

Bamu, B. N., Schauwer, E., & Hove, G. (2016). I can't say I wasn't anticipating it, but I didn't see it coming in this magnitude: A qualitative fieldwork experience in the northwest region of Cameroon. *The Qualitative Report, 21*(3), 571-583. Retrieved from https://nsuworks.nova.edu/tqr/

Bandura, A. (1989). Human agency in social cognitive theory. *American Psychologist, 44*(9), 1175-1184. doi:10.1037//0003-066X.44.9.1175

Barnard, M. (2016). How to apply for research ethics committee approval. *Nursing Children and Young People*, *28*(6), 16. doi:10.7748/ncyp.28.6.16.s20

Barratt, M. J., Ferris, J. A., & Lenton, S. (2015). Hidden populations, online purposive sampling, and external validity: Taking off the blindfold. *Field Methods,* 27, 1-19. doi:10.1177/1525822X14526838

Bartnes, M., Moe, N. B., & Heegaard, P. E. (2016). The future of information security incident management training: A case study of electrical power companies. *Computers & Security*, *61*(217528), 32-45. doi:10.1016/j.cose.2016.05.004

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

Bauer, S., & Bernroider, E. W. N. (2017). From information security awareness to reasoned compliant action: Analyzing information security policy compliance in a large banking organization. *Database for Advances in Information Systems*, *48*(3), 44-68. doi:10.1145/3130515.3130519.

Bauer, S., Bernroider, E. W. N., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers & Security*, *68*, 145-169. doi:10.1016/j.cose.2017.04.009

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

Bengtsson, M. (2016). How to plan and perform a qualitative study using content analysis. *Journal of Nursing Plus Open, 2*(2016), 8-14. doi:10.1016/j.npls.2016.01.001.

Bergmann, M. C., Dreißigacker, A., Von Skarczinski, B., & Wollinger, G. R. (2018). Cyber-dependent crime victimization: The same risk for everyone? *CyberPsychology, Behavior & Social Networking*, *21*(2), 84-90. doi:10.1089/cyber.2016.0727.

Bernik, I., & Prislan, K. (2016). Measuring information security performance with 10 by

10 model for holistic state evaluation. *PLoS One, 11,* doi:10.1371/journal.pone.0163050.

Beverland, M. B., Gemser, G., & Karpen, I. O. (2017). Design, consumption, and marketing: Outcomes, process, philosophy, and future directions. *Journal of Marketing Management, 33,* 59-172. doi:10.1080/0267257X.2017.1283908

Billen, A., Madrigal, J. A., Scior, K., Shaw, B. E., & Strydom, A. (2017). Donation of peripheral blood stem cells to unrelated strangers: A thematic analysis. *Plos ONE, 12*(10), 1-16. doi:10.1371/journal.pone.0186438

Biros, M. (2018). Capacity, vulnerability, and informed consent for research. *The Journal of Law, Medicine, & Ethics, 46,* 72-78. doi:10.1177110731051876602l.

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*(13), 1802–1811. doi:10.1177/1049732316654870.

Bliss, L. A. (2016). Phenomenological research: Inquiry to understand the meanings of people's experiences. *International Journal of Adult Vocational Education and Technology, 7*(3), 14-26. Retrieved from https://www.learntechlib.org/j/IJAVET/

Boddy, C. R. (2016). Sample size for qualitative research. *Qualitative Market Research: An International Journal, 19*(4), 426-432. doi:10.1108/qmr 06 2016 0053

Boeren, E. (2018). The methodological underdog: A review of quantitative research in the key adult education journals. *Adult Education Quarterly, 68*(1), 63-79. doi:10.1177/0741713617739347.

Boyaci, S. D. B., & Güner, M. (2018). The impact of authentic material use on

development of the reading comprehension, writing skills, and motivation in language course. *International Journal of Instruction*, *11*(2), 351–368. doi:10.12973/iji.2018.11224a

Brase, G. L., Vasserman, E. Y., & Hsu, W. (2017). Do different mental models influence cybersecurity behavior? Evaluations via statistical reasoning performance. *Frontiers in Psychology, 8*. doi:10.3389/fpsyg.2017.01929.

Bruce, A., Beuthin, R., Shields, L., Molzahn, A., & Schick-Mararoff, K. (2016). Narrative research evolving: Evolving through narrative research. *International Journal of Qualitative Methods, 15*(1), 1-6. doi:10.1177/1609406916659292.

Brusse, C., Kach, A. P., & Wagner, S. M. (2016). Boundary conditions: What they are, how to explore them, why we need them, and when to consider them. *Organizational Research Methods*, *20*(4), 574-609. doi:10.1177/1094428116641191.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-548. doi:10.2307/25750690

Burns, A. J., Posey, C., Roberts, T. L., & Lowry, P. B. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior, 68*, 190-209. doi:10.1016/j.chb.2016.11.018.

Camillo, M. (2017). Cybersecurity: Risks and management of risks for global banks and financial institutions. *Journal of Risk Management in Financial Institutions, 10*,

196–200. Retrieved from https://www.henrystewartpublications.com/jrm

Cardinale, I. (2018). Beyond constraining and enabling: Toward new microfoundations for institutional theory. *Academy of Management Review, 43*(1), 132-155. doi:10.5465/amr.2015.0020.

Carre, J. R., Curtis, S. R., & Jones, D. N. (2018). Ascribing responsibility for online security and data breaches. *Managerial Auditing Journal. 33*(4), 436-446, doi:10.1108/maj-11-2017-1693.

Castillo-Montoya, M. (2016). Preparing for interview research: The interview protocol refinement framework. *Qualitative Report, 21*(5), 811. Retrieved from https://nsuworks.nova.edu/tqr/

Cathro, V., O'Kane, P., & Gilbertson, D. (2017). Assessing reflection: Understanding skill development through reflective learning journals. *Education & Training, 59*(4), 427–442. doi.org/10.1108/ET-01-2017-0008

Chen, X., Chen, L., & Wu, D. (2018a). Factors that influence employees' security policy compliance: An awareness-motivation-capability perspective. *Journal of Computer Information Systems*, *58*(4), 312-324, doi:10.1080/08874417.2016.1258679

Chen, X., Wu, D., Chen, L., & Teng, J. K. L. (2018b). Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables. *Information & Management*, *55*, 1049–1060. doi:10.1016/j.im.2018.05.011.

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS

security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security, 39*(PART B), 447-459. doi:10.1016/j.cose.2013.09.009.

Choi, M. (2016). Leadership of information security manager on the effectiveness of information systems security for secure sustainable computing. *Sustainability, 8*(7), 638. doi:10.3390/su8070638.

Christensen, P. H., Robinson, S., & Simons, R. A. (2016). The application of mixed methods: using a crossover analysis strategy for product development in real estate. *Journal of Real Estate Literature, 24*(2), 429-451. doi: 10.1080/10835547.2016.12090436

Chua, H. N., Wong, S. F., Low, Y. C., & Chang, Y. (2018). Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations. *Telematics and Informatics, 35*(6), 1770-1780. doi:10.1016/j.tele.2018.05.005

Chul Ho, L., Xianjun, G., & Raghunathan, S. (2016). Mandatory standards and organizational information security. *Information Systems Research, 27*(1), 70-86. doi:10.1287/isre.2015.0607.

Civitillo, S., Juang, L. P., Badra, M., & Schachner, M. K. (2019). The interplay between culturally responsive teaching, cultural diversity beliefs, and self-reflection: A multiple case study. *Teaching and Teacher Education, 77*, 341–351. doi:10.1016/j.tate.2018.11.002

Clark, K. R., & Vealé, B. L. (2018). Strategies to enhance data collection and analysis in

qualitative research. *Radiologic Technology*, *89*(5), 482CT–485CT. Retrieved from http://www.radiologictechnology.org/

Clemons, E. K., Dewan, R. M., Kauffman, R. J., & Weber, T. A. (2017). Understanding the information-based transformation of strategy and society. *Journal of Management Information Systems,* 34(2), 425–456. doi:10.1080/07421222.2017.1334474

Cong, H., Dang, D., Brennan, L., & Richardson, J. (2017). Information security and people: A conundrum for compliance. *Australasian Journal of Information Systems,* 21, 1-16. doi:10.3127/ajis.v21i0.1321

Connelly, L. M. (2016). Trustworthiness in qualitative research. *Medsurg Nursing, 25*(6), 435-436. Retrieved from www.medsurgnursing.net

Conner, M., McEachan, R., Taylor, N., O'Hara, J., & Lawton, R. (2015). Role of affective attitudes and anticipated affective reactions in predicting health behaviors. *Health Psychology*, 34(6), 642. doi:10.1037/hea0000143.

Connolly, L. Y., Lang, M., Gathegi, J., & Tygar, D. J. (2017). Organisational culture, procedural countermeasures, and employee security behaviour: A qualitative study. *Information & Computer Security*, *25*, 118-136. doi:10.1108/ICS-03-2017-0013

Cooper, M. (2016). Adventures in Ethical Hacking. *ITNOW*, *58*(3), 36-37. doi:10.1093/itnow/bww074

Cox, J. A. (2012). *Organizational narcissism as a factor in information security: A structured model of the user knowing-doing gap.* Capella University

(Dissertation). Retrieved from ProQuest Dissertations & Theses Global database. (UMI No. 3499909).

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

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

Cuganesan, S., Steele, C., & Hart, A. (2018). How senior management and workplace norms influence information security attitudes and self-efficacy. *Behavior and Information Technology*, *37*(1), 50-65. doi:10.1080/0144929X.2017.1397193

Curran, T. (2015). Information security (IS) training: Instructional design project. *Journal of Applied Learning Technology, 5*(3), 24-30. Retrieved from http://lti.org

Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2017). Why employees share information security advice? Exploring the contributing factors and structural patterns of security advice sharing in the workplace. *Computers in Human Behavior, 67,* 196-206. doi:10.1016/j.chb.2016.10.025.

D'Arcy, J., & Lowry, P. B. (2017). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal*. *29*(1), 43-69, doi:10.1111/isj.12173.

Das, A., & Khan, H. U. (2016). Security behaviors of smartphone users. *Information &*

Computer Security, *24*(1), 116–134. doi:10.1108/ICS-04-2015-0018

Da Veiga, A. (2016). Comparing the information security culture of employees who had read the information security policy and those who had not: Illustrated through an empirical study, *Information & Computer Security*, *24*(2), 139-151. doi:10.1108/ICS-12-2015-0048.

Da Veiga, A., & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. *Computers & Security*, *70*, 72-94. doi:10.1016/j.cose.2017.05.002

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, *13*(3), 319-340. doi:10.2307/249008

De Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, *34*(1), 1-7. doi:10.1016/j.giq.2017.02.007

Dhillon, G., Syed, R., & Pedron, C. (2016). Interpreting information security culture: An organizational transformation case study. *Computers & Security, 56*, 63-69. doi:10.1016/j.cose.2015.10.001.

Dikko, M. (2016). Establishing construct validity and reliability: Pilot testing of a qualitative interview for research in Takaful (Islamic Insurance). *Qualitative Report*, *21*(3), 521-528. Retrieved from https://nsuworks.nova.edu/tqr/

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organization fields. *American Sociological Review*, *48*(2), 147-160. doi:10.2307/2095101.

Doherty, N. F., & Tajuddin, S. T. (2018). Towards a user-centric theory of value-driven information security compliance. *Information Technology & People, 31*(2), 348–367. doi:10.1108/ITP-08-2016-0194

Donald, I. J., Cooper, S. R., & Conchie, S. M. (2014). An extended theory of planned behaviour model of the psychological factors affecting commuters' transport mode use. *Journal of Environmental Psychology, 40,* 39-48. doi:10.1016/j.jenvp.2014.03.003

Ebneyamini, S., & Moghadam, M. R. S. (2018). Toward developing a framework for conducting case study research. *International Journal of Qualitative Methods,* 17, 1-11. doi: 10.1177/1609406918817954.

El Hussein, M. T., Jakubec, S. L., & Osuji, J. (2016). The FACTS: A mnemonic for the rapid assessment of rigor in qualitative research studies. *Journal of Nursing Education*, *55*(1), 60–60. doi:10.3928/01484834-20151214-15

Elifoglu, H., Abel, I., & Tasseven, O. (2018). Minimizing insider threat risk with behavioral monitoring. *Review of Business, 38*(2), 61-73. Retrieved from https://www.stjohns.edu/academics/schools/peter-j-tobin-college-business/departments-faculty/review-business

Elkhannoubi, H., & Belasissaoui, M. (2016). A framework for an effective cybersecurity strategy implementation. *Journal of Information Assurance & Security*, *11(*4), 233–241. Retrieved from http://www.mirlabs.org/jias/

El-Masri, M. M. (2017). Non-probability sampling: The process of selecting research participants non-randomly from a target population. *Canadian Nurse, 113*(3), 17.

Retrieved from https://www.canadian-nurse.com/

El Said, G. R. (2017). Understanding how learners use massive open online courses and why they drop out: Thematic analysis of an interview study in a developing country. *Journal of Educational Computing Research*, *55*(5), 724-752. doi:10.1177/0735633116681302

Esteves, J., Ramalho, E., & De Haro, G. (2017). To improve cybersecurity, think like a hacker. *MIT Sloan Management Review*, *58*(3), 71. Retrieved from https://sloanreview.mit.edu/

Estevez, E., Janowski, T., & Lopes, N. V. (2016). Policy monitoring on accessible technology for inclusive education - Research findings and requirements for a software tool. *Journal of Computer Science & Technology*, *16*(1), 29-37. Retrieved from http://journal.info.unlp.edu.ar/JCST/

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), 1-4. doi:10.11648/j.ajtas.20160501.11

Evans, M., Maglaras, L. A., He, Y., & Janicke, H. (2016). Human behavior as an aspect of cybersecurity assurance. *Security and Communication Networks, 9*(17), 4667-4679. doi:10.1002/sec.1657

Faronbi, J. O., Faronbi, G. O., Ayamolowo, S. J., & Olaogun, A. A. (2019). Caring for the seniors with chronic illness: The lived experience of caregivers of older adults. *Archives of Gerontology and Geriatrics, 82*, 8–14. doi:10.1016/j.archger.2019.01.013.

Ferreira, R. J., Buttell, F., & Ferreira, S. B. (2015). Ethical Considerations for Conducting Disaster Research with Vulnerable Populations. *Journal of Social Work Values and Ethics, 12*(1), 29–40. Retrieved from https://jswve.org/

Fielding, J. (2019). Back to basics: Tackling security threats in an increasingly complex world. *Computer Fraud & Security, 2019(7),* 6-8. doi:10.1016/S1361-3723(19)30072-7.

Fishbein, M. (1967). A behavior theory approach to the relations between beliefs about an object and the attitude toward the object. In M. Fishbein (Ed.), *Readings in attitude theory and measurement* (pp. 389-400). New York: John Wiley & Sons.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research*. Reading, MA: Addison-Wesley.

FitzPatrick, B. (2019). Validity in qualitative health education research. *Currents in Pharmacy Teaching and Learning*, *11*(2), 211–217. doi:10.1016/j.cptl.2018.11.014.

Florencio, D., Herley, C., & Van Oorschot, P. C. (2016). Pushing on String: The 'Don't Care' Region of Password Strength. *Communications of the ACM, 59*(11), 66-74. doi:10.1145/2934663.

Flores, W. R., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture, and awareness. *Computers & Security, 59,* 26. doi:10.1016/j.cose.2016.01.004.

Flowerday, S. V., & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how, and who. *Computers & Security, 61,* 169-183.

doi:10.1016/j.cose.2016.06.002.

Font, X., Garay, L., & Jones, S. (2016). A social cognitive theory of sustainability empathy. *Annals of Tourism Research, 58,* 65-80. doi:10.1016/j.annals.2016.02.004

Forero, R., Nahidi, S., De Costa, J., Mohsin, M., Fitzgerald, G., Gibson, N., … Aboagye-Sarfo, P. (2018). Application of four-dimension criteria to assess rigour of qualitative research in emergency medicine. *BMC Health Services Research, 18*(1), 120. doi:10.1186/s12913-018-2915-2

Forster, D. G., & Borasky, D. (2018). Adults lacking capacity to give consent when is it acceptable to include them in research. *Therapeutic Innovation & Regulatory Science, 52*(3), 275-279. doi:10.1177/2168479018770658.

Fritz, J., & Kaefer, F. (2017). The rise of the mega-breach and what can be done about it. *Journal of Applied Security Research, 12*(3), 392-406. doi:10.1080/19361610.2017.1315700.

Fusch, P. I., Fusch, G. E., & Ness, L. R. (2017). How to conduct a mini-ethnographic case study: A guide for novice researchers. *The Qualitative Report, 22*(3), 923-941. Retrieved from https://nsuworks.nova.edu/tqr/

Galinec, D., Možnik, D., & Guberina, B. (2017). Cybersecurity and cyber defense: National level strategic approach. *Automatika: Journal for Control, Measurement, Electronics, Computing & Communications, 58,* 273-286. doi:10.1080/00051144.2017.1407022

Gelinas, L., Wertheimeir, A., & Miller, F. G. (2016). When and why is research without

consent permissible? *Hastings Center Report*, *46*(2), 35-43. doi:10.1002/hast.548.

Gentles, S. J., Charles, C., Ploeg, J., & McKibbon, K. A. (2015). Sampling in qualitative research: Insights from an overview of the methods literature. *The Qualitative Report*, 20, 1772-1789. Retrieved from https://nsuworks.nova.edu/tqr/

Gerhold, L., Bartl, G., & Haake, N. (2017). Security culture 2030: How security experts assess the future state of privatization, surveillance, security technologies, and risk awareness in Germany. *Futures, 87*, 50-64. doi:10.1016/j.futures.2017.01.005

Gheyas, A., & Abdallah, E. (2016). Detection and prediction of insider threats to cybersecurity: a systematic literature review and meta-analysis. *Big Data Analytics, 1*(1), 6. doi:10.1186/s41044-016-0006-0.

Ghorbel, A., Ghorbel, M., & Jmaiel, M. (2017). Privacy in cloud computing environments: A survey and research challenges. *Journal of Supercomputing*, *73*(6), 2763-2800. doi:10.1007/s11227-016-1953-y.

Gibson, C. B. (2017). Elaboration, generalization, triangulation, and interpretation: On enhancing the value of mixed-method research. *Organizational Research Methods, 20*(2), 193-223. doi:10.1177/1094428116639133.

Giles, E. L., Becker, F., Ternent, L., Sniehotta, F. F., McColl, E., & Adams, J. (2016). Acceptability of financial incentives for health behaviours: A discrete choice experiment. *PLoS One, 11*(6), 1-19. doi:10.1371/journal.pone

Goel, D., & Jain, A. K. (2017). Mobile phishing attacks and defense mechanisms: state of the art and open research challenges. *Computers & Security, 73*, 519-544. doi:10.1016/j.cose.2017.12.006.

Grobler, J. (2018). Cyber risk from a chief risk officer perspective. *Journal of Risk Management in Financial Institutions, 11*(2), 125. Retrieved from https://www.henrystewartpublications.com/jrm

Guo, Y., & Zhang, Z. (2017). LPSE: lightweight password-strength estimation for password meters. *Computers & Security, 73*, 507-518. doi:10.1016/j.cose.2017.07.012

Gurung, A., & Raja, M. K. (2016). Online privacy and security concerns of consumers. *Information and Computer Security*, *24*(4), 348–371. doi:10.1108/ICS-05-2015-0020.

Hadlington, L. (2018). The human factor in cybersecurity: Exploring the accidental insider. *In Psychological and Behavioral Examinations in Cyber Security*, 46-63. Hershey, PA: IGI Global. doi:10.4018/978-1-5225-4053-3.ch003

Hagaman, A. K., & Wutich, A. (2017). How many interviews are enough to identify metathemes in multisited and cross-cultural research? Another perspective on Guest, Bunce, & Johnson's (2006) landmark study. *Field Methods, 29*(1), 23-41. doi:10.1177/1525822X16640447

Hall, M. (2016). Feature: Why people are key to cyber-security. *Network Security, 2016*, 9-10. doi:10.1016/S1353-4858(16)30057-5.

Hammer, M. J. (2016). Informed consent in the changing landscape of research. *Oncology Nursing Forum, 43*(5), 558. doi:10.1188/16.ONF.558-560.

Han, J. Y., Kim, Y. J., & Kim, H. (2017). An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective.

Computers & Security, *66*, 52–65. doi:10.1016/j.cose.2016.12.016

Hancock, M. E., Amankwaa, L., Revell, M. A., & Mueller, D. (2016). Focus group data saturation: A new approach to data analysis. *Qualitative Report, 21*(11), 2124. Retrieved from https://nsuworks.nova.edu/tqr/

Handwerker, S. M. (2018). Challenges experienced by nursing students overcoming one course failure: A phenomenological research study. *Teaching and Learning in Nursing*, *13*, 168-173. doi:10.1016/j.teln.2018.03.007.

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

Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computers & Security*, *73*, 102-113. doi:10.1016/j.cose.2017.10.008

Haydon, G., Browne, G., & Van der Riet, P. (2018). Narrative inquiry as a research methodology exploring person centred care in nursing. *Collegian, 25*(1), 125-129. doi:10.1016/j.colegn.2017.03.001

He, W., & Zhang, Z. (2019). Enterprise cybersecurity training and awareness programs: Recommendations for success. *Journal of Organizational Computing and Electronic Commerce*, 1-9. doi:10.1080/10919392.2019.1611528

Heartfield, R., & Loukas, G. (2018). Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework. *Computers & Security, 76*, 101-127. doi:10.1016/j.cose.2018.02.020

Heetae, Y., Hwansoo, J., & Hangjung, Z. (2017). User acceptance of smart home services: An extension of the theory of planned behavior. *Industrial Management & Data Systems,* 117(1), 68-89. doi: 10.1108/IMDS-01-2016-0017

Heickero, R. (2016). Cyber espionage and illegitimate information retrieval. *International Journal of Cyber Warfare and Terrorism, 6*(1), 13-23. doi:10.4018/ijcwt.2016010102.

Helil, N., & Rahman, K. (2017). CP-ABE access control scheme for sensitive data set constraint with hidden access policy and constraint policy. *Security and Communication Networks, 2017*. doi:10.1155/2017/2713595.

Hemphill, T. A., & Longstreet, P. (2016). Financial data breaches in the U.S. retail economy: Restoring confidence in information technology security standards. *Technology in Society, 44*, 30-38. doi:10.1016/j.techsoc.2015.11.007

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organizations. *European Journal of Information Systems, 18*(2), 106-125. doi:10.1057/ejis.2009.6.

Hills, M., & Anjali, A. (2017). A human factors contribution to countering insider threats: Practical prospects from a novel approach to warning and avoiding. *Security Journal, 30*(1), 142-152. doi:10.1057/sj.2015.36.

Hina, S., Selvam, D. D. D. P., & Lowry, P. B. (2019). Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world. *Computers & Security, 87*, 1-15, doi:10.1016/j.cose.2019.101594.

Hofeditz, M., Nienaber, A. M., Dysvik, A., & Schewe, G. (2017). "Want to" versus "have to": Intrinsic and extrinsic motivators as predictors of compliance behavior intention. *Human Resource Management*, *56*(1), 25-49. doi:10.1002/hrm.21774

Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., & Ochoa, M. (2019). Insight into insiders and it: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. *ACM Computing Surveys (CSUR)*, *52*(2), 30-84. doi:10.1145/3303771.

Hoover, S. M., Strapp, C. M., Ito, A., Foster, K., & Roth, K. (2018). Teaching qualitative research interviewer skills: A developmental framework for social justice psychological research teams. *Qualitative Psychology*, *5*(2), 300–318. doi:10.1037/qup0000101.

Horne, C. A., Maynard, S. B., & Ahmad, A. (2017). Organizational information security strategy: Review, discussion, and future research. *Australasian Journal of Information Systems*, *21*, 1-17. doi:10.3127/ajis.v21i0.1427.

Hu, P. J., Hu, H., Wei, C., & Hsu, P. (2016). Examining firms' green information technology practices: A hierarchical view of key drivers and their effects. *Journal of Management Information Systems*, *33*(4), 1149-1179. doi:10.1080/07421222.2016.1267532.

Humaidi, N., & Balakrishnan, V. (2018). Indirect effect of management support on users' compliance behaviour towards information security policies. *Health Information Management Journal*, *47*(1), 17–27. doi 10.1177/1833358317700255.

Hwang, I., & Cha, O. (2018). Examining technostress creators and role stress as potential

threats to employees' information security compliance. *Computers in Human Behavior*, *81*, 282-293. doi:10.1016/j.chb.2017.12.022

Hwang, I., Kim, D., Kim, T., & Kim, S. (2017). Why not comply with information security? An empirical approach for the causes of noncompliance. *Online Information Review*, *41*(1), 2-18. doi:10.1108/oir-11-2015-0358.

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information and Management, 51*(1), 69-79. doi:10.1016/j.im.2013.10.001.

Ifinedo, P. (2016). Critical times for organizations: What should be done to curb workers' noncompliance with IS security policy guidelines? *Information Systems Management*, *33*(1), 30-41. doi:10.1080/10580530.2015.1117868.

Iivari, N. (2018). Using member checking in interpretive research practice: A hermeneutic analysis of informants' interpretation of their organizational realities. *Information Technology & People*, 31(1), 111-113. doi:10.1108/ITP-07-2016-0168.

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

Jalali, M. S., Bruckes, M., Westmattelmann, D., & Schewe, G. (2020). Why employees (still) click on phishing links: Investigation in hospitals. *Journal of Medical Internet Research, 22*(1), 1-16. doi:10.2196/16775.

James, N. (2017). Using narrative inquiry to explore the experience of one ethnically diverse ESL nursing student. *Teaching and Learning in Nursing*, 1-6. doi:10.1016/j.teln.2017.08.002

Jansen, J., & Van Schaik, P. (2017). Comparing three models to explain precautionary online behavioral intentions. *Information and Computer Security, 25*(2), 165-180. doi:10.1108/ICS-03-2017-0018.

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

Jeong, C. Y., Lee, S. T., & Lim, J. (2019). Information security breaches and IT security investments: Impacts on competitors. *Information & Management*, *56*, 681–695. doi:10.1016/j.im.2018.11.003

Jeske, D., & Van Schaik, P. (2017). Familiarity with Internet threats: Beyond awareness. *Computers & Security*, 66, 129–141. doi: 10.1016/j.cose.2017.01.010.

Jiang, K., Ling, F., Feng, Z., Wang, K., & Guo, L. (2017). Psychological predictors of mobile phone use while crossing the street among college students: An application of the theory of planned behavior. *Traffic Injury Prevention, 18*(2), 118-123. doi:10.1080/15389588.2016.1236195.

Johnston, A. C., Warkentin, M., Mcbride, M., & Carter, L. (2016). Dispositional and situational factors: Influences on information security policy violations. *European Journal of Information Systems, 25*(3), 231-251. doi:10.1057/ejis.2015.15.

Joshi, C., & Singh, U. K. (2017). Information security risks management framework – A

step towards mitigating security risks in university network. *Journal of Information Security and Applications, 35*, 128-137. doi:10.1016/j.jisa.2017.06.006.

Joslin, R., & Muller, 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.

Karlsson, F., Hedstrom, K., & Goldkuhl, G. (2017). Practice-based discourse analysis of information security policies. *Computers & Security, 67*, 267-279. doi:10.1016/j.cose.2016.12.012.

Kasdan, D. O. (2016). Public administration, social progress, and the utopian null: reconfiguring the hypothesis test for neopragmatist bureaucracy. *International Review of Public Administration, 21*(2), 163-175. doi:10.1080/12294659.2016.1186456

Ke, L. (2016). Integrating ethical guidelines and situated ethics for researching social-media-based interactions. *Journal of Information Ethics, 25*(1), 114-131. https://mcfarlandbooks.com/product/journal-of-information-ethics-vol-25-no-1-spring-2016/

Kearney, W. D., & Kruger, H. A. (2016). Can perceptual differences account for enigmatic information security behavior in an organization? *Computers & Security*, *61*, 46–58. doi:10.1016/j.cose.2016.05.006.

Kerwin-Boudreau, S., & Butler-Kisber, L. (2016). Deepening understanding in qualitative inquiry. *Qualitative Report, 21*(5), 956-971. Retrieved from

https://nsuworks.nova.edu/tqr/

Ki-Aries, D., & Faily, S. (2017). Persona-centred information security awareness. *Computers & Security, 70*, 663-674. doi: 10.1016/j.cose.2017.08.001.

Kim, H. L., & Han, J. (2019). Do employees in a good company comply better with information security policy? : A corporate social responsibility perspective. *Information Technology & People*, *32*(4), 858-875. doi:10.1108/ITP-09-2017-0298.

Kim, S., Kim, G., & French, A. (2015). Relationships between need-pull/technology-push and information security management and the moderating role of regulatory pressure. *Information Technology & Management, 16*(3), 173-192. doi:10.1007/s10799-015-0217-5

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

King, K. M., Pullmann, M. D., Lyon, A. R., Dorsey, S., & Lewis, C. C. (2019). Using implementation science to close the gap between the optimal and typical practice of quantitative methods in clinical science. *Journal of Abnormal Psychology*, *128*(6), 547–562. doi:10.1037/abn0000417.

Klein, R. H., & Luciano, E. M. (2016). What influences information security behavior? A study with brazilian users. *Journal of Information Systems and Technology Management*, *13*(3), 479–496. doi:10.4301/S1807-17752016000300007.

Kline, T. J. B. (2017). Sample issues, methodological implications, and best practices.

Canadian Journal of Behavioural Science, *49*(2), 71-77. doi:10.1037/cbs0000054.

Koohikamali, M., Peak, D. A., & Prybutok, V. R. (2017). Beyond self-disclosure: Disclosure of information about others in social network sites. *Computers in Human Behavior*, *69*, 29-42. doi:10.1016/j.chb.2016.12.012

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

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

Krajnović, D. M., & Jocić, D. D. (2017). Experience and attitudes toward informed consent in pharmacy practice research: Do pharmacists care? *Science and Engineering Ethics*, *23*(6), 1529–1539. doi:10.1007/s11948-016-9853-3.

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, *25*(1), 1-10. doi:10.3233/thc-161263.

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

Lasrado, F., & Uzbeck, C. (2017). The excellence quest: a study of business excellence

award-winning organizations in UAE. *Benchmarking: An International Journal*, *24*(3), 716-734. doi:10.1108/BIJ-06-2016-0098.

Laube, S., & Bohme, R. (2016). The economics of mandatory security breach reporting to authorities. *Journal of Cybersecurity*, *2*(1), 29-41. doi:10.1093/cybsec/tyw002.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. H. (2014). Information security awareness and behavior: a theory-based literature review. *Management Research Review*, *37*(12), 1049-1092. doi:10.1108/MRR-04-2013-0085

Lee, C., Lee, C. C., & Kim, S. (2016a). Understanding information security stress: Focusing on the type of information security compliance activity. *Computers & Security*, *59*, 60-70. doi:10.1016/j.cose.2016.02.004.

Lee, N., Li, S., Shin, B., & Kwon, O. (2016b). Social comparison, goal contagion, and adoption of innovative information technology. *Journal of Computer Information Systems, 56*(2), 127-136. doi:10.1080/08874417.2016.1117374

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

Lopes, I. M., & Sá-Soares, F. d. (2014). Institutionalization of information systems security policies adoption: Factors and guidelines. *IADIS International Journal on Computer Science & Information Systems*, *9(*2), 82-95. Retrieved from http://www.iadisportal.org/ijcsis/

Lowe, A., Norris, A. C., Farris, A. J., & Babbage, D. R. (2018). Quantifying thematic

saturation in qualitative data analysis. *Field Methods*, *30*(3), 191–207. doi:10.1177/1525822X17749386.

Luna, R., Rhine, E., Myhra, M., Sullivan, R., & Kruse, C. S. (2016). Cyber threats to health information systems: A systematic review. *Technology and Healthcare*, *24*(1), 1-9. doi:10.3233/thc151102.

Lykou, G., Anagnostopoulou, A., & Gritzalis, D. (2019). Smart airport cybersecurity: Threat mitigation and cyber resilience controls. *Sensors, 19*(1), 19, doi:10.3390/s19010019

Madden, T. J., Ellen, P. S., & Ajzen, I. (1992). A comparison of the theory of planned behavior and the theory of reasoned action. *Personality and Social Psychology Bulletin, 18*(1), 3-9. doi:10.1177/0146167292181001

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*(1), 1-12. doi:10.1177/1609406918786362

Mahmood, J., Dahlan, H. M., Hussin, A. R. C., & Ahmad, M. A. (2016). Review on knowledge sharing behavior studies: Theories and research approaches. *Indian Journal of Science and Technology*, *9*(34). doi: 10.17485/ijst/2016/v9i34/100834.

Mailloux, L. O., & Grimaila, M. (2018). Advancing cybersecurity: The growing need for a cyber-resiliency workforce. *IT Professional, 20*, 23-30. doi:10.1109/MITP.2018.032501745.

Malterud, K., Siersma, V. D., & Guassora, A. D. (2016). Sample size in qualitative

interview studies. *Qualitative Health Research, 26*(13), 1753-1760. doi:10.1177/1049732315617444.

Mamonov, S., & Benbunan-Fich, R. (2018). The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior, 83,* 32-44. doi:10.1016/j.chb.2018.01.028

Manworren, N., Letwat, J., & Daily, O. (2016). Why you should care about the target data breach. *Business Horizons, 59*(3), 257-266. doi:10.1016/j.bushor.2016.01.002.

Maramwidze-Merrison, E. (2016). Innovative methodologies in qualitative research: Social media window for accessing organizational elites for interviews. *Electronic Journal of Business Research Methods*, *14*(2), 157-167. Retrieved from http://www.ejbrm.com/main.html

Marshall, C., & Rossman, G. (2016). *Designing qualitative research (*6th ed.). Washington, DC: Sage.

Mayer, P., Gerber, N., McDermott, R., Volkamer, M., & Vogt, J. (2017). Productivity vs security: mitigating conflicting goals in organizations. *Information and Computer Security*, *5*(2), 137-151. doi:10.1108/ICS-03-2017-0014

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior, 69,* 151–156. doi:10.1016/j.chb.2016.11.065.

McFadyen, J., & Rankin, J. (2016). The role of gatekeepers in research: Learning from reflexivity and reflection. *GSTF Journal of Nursing and Health Care*

(JNHC), *4*(1), 82-88. doi:10.5176/2345-718X_4.1.135.

McGovern, T., Small, A., & Hicks, C. (2017). Diffusion of process improvement methods in European SMEs. *International Journal of Operations & Production Management, 37*(5), 607-629. doi:10.1108/IJOPM-11-2015-0694.

Mehraeen, E., Ghazisaeedi, M., Farzi, J., & Mirshekari, S. (2016). Security challenges in healthcare cloud security: A systematic review. *Global Journal of Health Science*, *9*(3), 157-166. doi:10.5539/gjhs.v9n3p157.

Menard, P., Bott, G. J., & Crossler, R. E. (2017). User motivations in protecting information security: Protection motivation theory versus self-determination theory. *Journal of Management Information Systems, 34*(4), 1203-1230. doi:10.1080/07421222.2017.1394083

Miranda, M. J. (2018). Enhancing cybersecurity awareness training: A comprehensive phishing exercise approach. *International Management Review, 14*(2), 5-10. Retrieved from https://www.questia.com/library/p150683/international-management-review

Mohajan, H. K. (2018). Qualitative research methodology in social sciences and related subjects. *Journal of Economic Development, Environment, and People*, *7*(1), 23. doi:10.26458/jedep.v7i1.571

Mohamed, I. A. H. (2017). Some issues in the institutional theory: A critical analysis. *International Journal of Scientific & Technology Research*, *6*(9), 150-156. Retrieved from https://www.ijstr.org/

Mol, A. M., Silva, R. S., Rocha, Á. A., & Ishitani, L. (2017). Ethnography and

Phenomenology applied to game research: a systematic literature review. *Revista De Sistemas E Computação (RSC), 7*(2), 110-127. Retrieved from https://revistas.unifacs.br/

Molin, E., Meeuwisse, K., Pieters, W., & Chorus, C. (2018). Secure or usable computers? Revealing employees' perceptions and trade-offs by means of a discrete choice experiment. *Computers & Security, 77*, 65-78. doi:10.1016/j.cose.2018.03.003

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly, 42*(1), 285-308. doi:10.25300/MISQ/2018/13853.

Morar, P., Read, J., Arora, S., Hart, A., Warusavitarne, J., Green, J., … Faiz, O. (2016). Defining the optimal design of the inflammatory bowel disease multidisciplinary team: Results from a multicentre qualitative expert-based study. *Frontline Gastroenterology, 6*(4), 290-297. doi:10.1136/flgastro-2014-100549.

Mortenson, M. J., & Vidgen, R. (2016). A computational literature review of the technology acceptance model. *International Journal of Information Management, 36*(6, 1248–1259. doi:10.1016/j.ijinfomgt.2016.07.007

Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates, and scenarios. *Computers & Security, 59*, 186-209. doi:10.1016/j.cose.2016.03.004

Mwagwabi, F., McGill, T., & Dixon, M. (2014). Improving compliance with password guidelines: How user perceptions of passwords and security threats affect compliance with guidelines. *In 2014 47th Hawaii International Conference on*

System Sciences (pp. 3188-3197). IEEE. doi:10.1109/hicss.2014.396

Nebeker, C., Lagare, T., Takemoto, M., Lewars, B., Crist, K., Bloss, C. S., & Kerr, J. (2016). Engaging research participants to inform the ethical conduct of mobile imaging, pervasive sensing, and location tracking research. *Translational Behavioral Medicine, 6*(4), 577-586. doi:10.1007/s13142-016-0426-4

Nelson, A. M. (2016). Methodology for examining attributes of African Americans in the department of defense senior executive service Corp. *Journal of Economic Development, Management, IT, Finance & Marketing*, *8*(1), 48-68. Retrieved from https://gsmi-ijgb.com/?page_id=81

Niblett, G. (2016). Insider Threats. *ITNow*, *58*(2), 23. doi:10.1093/itnow/bww039

Niemimaa, E., & Niemimaa, M. (2017). Information systems security policy implementation in practice: from best practices to situated practices. *European Journal of Information Systems, 26*(1), 1-20. doi:10.1057/s41303-016-0025-y

Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. *Holistica*, 9(3), 71-88. doi:10.2478/hjbpa-2018-0024

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*(1), 1-13. doi:10.1177/1609406917733847

Ntinda, K., Ntinda, M. N., & Mpofu, E. (2017). Teacher-reported quality of schooling indicators in Botswana primary schools: An exploratory study. *Perspectives in Education*, *33*(1), 117-130. Retrieved from https://journals.ufs.ac.za/

Ogutcu, G., Testik, O. M., & Chouseinoglou, O. (2016). Analysis of personal information

security behavior and awareness. *Computers & Security*, *56*, 83–93. doi:10.1016/j.cose.2015.10.002.

Omar, M., Mohammed, D., & Nguyen, V. (2017). Defending against malicious insiders: A conceptual framework for predicting, detecting, and deterring malicious insiders. *International Journal of Business Process Integration and Management, 8*, 114-119. doi:10.1504/IJBPIM.2017.083794

Opderbeck, D. W. (2016). Cybersecurity, data breaches, and the economic loss doctrine in the payment card industry. *Maryland Law Review*, *75*(4), 935. doi:10.2139/ssrn.2636944.

Park, E. H., Kim, J., & Park, Y. S. (2017a). The role of information security learning and individual factors in disclosing patients' health information. *Computers & Security*, *65*, 64-76. doi:10.1016/j.cose.2016.10.011

Park, S. H., Hsieh, C. M., & Lee, C. K. (2017b). Examining chinese college students'intention to travel to Japan using the extended theory of planned behavior: Testing destination image and the mediating role of travel constraints. *Journal of Travel & Tourism Marketing, 34*(1), 113-131. doi:10.1080/10548408.2016.1141154.

Patino, C. M., & Ferreira, J. C. (2018). Internal and external validity: can you apply research study results to your patients? *Jornal Brasileiro De Pneumologia*, *44*(3), 183. doi:10.1590/S1806-37562018000000164.

Paul, J., Modi, A., & Patel, J. (2016). Predicting green product consumption using theory of planned behavior and reasoned action. *Journal of Retailing and Consumer*

Services, 29, 123-134. doi:10.1016/j.jretconser.2015.11.006.

Peck, B., & Mummery, J. (2017). Hermeneutic constructivism: An ontology for qualitative research. *Qualitative Health Research, 28*(3), 389–407. doi:10.1177/1049732317706931.

Perrault, E. K. (2018). Using an interactive online quiz to recalibrate college students' attitudes and behavioral intentions about phishing. *Journal of Educational Computing Research, 55*(8), 1154-1167. doi:10.1177/0735633117699232.

Peticca-Harris, A., DeGama, N., & Elias, S. R. (2016). A dynamic process model for finding informants and gaining access in qualitative research. *Organizational Research Methods, 19*(3), 376-401. doi:10.1177/1094428116629218.

Pham, H. C., El-Den, J., & Richardson, J. (2016). Stress-based security compliance model - an exploratory study. *Information and Computer Security*, *24*(4), 326-347. doi:10.1108/ICS-10-2014-0067.

Pham, H. C., Pham, D. D., Brennan, L., & Richardson, J. (2017). Information security and people: A conundrum for compliance. *Australasian Journal of Information Systems, 21*. doi:10.3127/ajis.v21i0.1321

Pipa, M. D., & Sirbu, J. (2016). Organizational communication from the perspective of qualitative analysis. *Calitatea, 17*(2), 58-68. Retrieved from https://www.srac.ro/calitatea/

Popescul, L. F., & Jitaru, L. (2017). Research methods used in studies on management and international affairs. *Journal of Public Administration, Finance & Law, 2017(*11), 157-162. Retrieved from http://www.jopafl.com/

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems, 57,* 338-349. doi:10.1080/07421222.2015.1138374

Posner, B. Z. (2016). Investigating the reliability and validity of the leadership practices inventory. *Administrative Sciences,* 6(4), 1-23. doi:10.3390/admsci6040017.

Prapavessis, H., Gaston, A., & DeJesus, S. (2015). The theory of planned behavior as a model for understanding sedentary behavior. *Psychology of Sport and Exercise, 19,* 23-32. doi:10.1016/j.psychsport.2015.02.001

Pussewalage, H. S. G., & Oleshchuk, V. A. (2016). Privacy preserving mechanisms for enforcing security and privacy requirements in E-health solutions. *International Journal of Information Management*, *36*(6), 1161-1173. doi:10.1016/j.ijinfomgt.2016.07.006.

Rahi, S. (2017). Research design and methods: A systematic review of research paradigms, sampling issues, and instruments development. *International Journal of Economics & Management Sciences*, *6*(2), 1-5. doi: 10.4172/2162-6359.100040.

Rajab, M., & Eydgahi, A. (2019). Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. *Computers & Security*, *80,* 211–223, 2019. doi 10.1016/j.cose.2018.09.016.

Ranjan, P., & Om, H. (2016). An efficient remote user password authentication scheme

based on Rabin's Cryptosystem. *Wireless Personal Communications*, *90*(1), 217-244. doi:10.1007/s11277-016-3342-5.

Renz, S. M., Carrington, J. M., & Badger, T. A. (2018). Two strategies for qualitative content analysis: An intramethod approach to triangulation. *Qualitative Health Research, 28*(5), 824-831. doi:10.1177/1049732317753586.

Ridder, H. (2017). The theory contribution of case study research designs. *Business Research, 10*, 281-305. doi:10.1007/s40685-017-0045-z

Ritzman, M. E., & Kahle-Piasecki, L. (2016). What works: A systems approach to employee performance in strengthening information security. *Performance Improvement, 55*(8), 17-22. doi:10.1002/pfi.21614.

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

Rolbiecki, A., Subramanian, R., Crenshaw, B., Albright, D. L., Perreault, M., & Mehr, D. (2017). A qualitative exploration of resilience among patients living with chronic pain. *Traumatology, 23*(1), 89. doi: 10.1037/trm0000095

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

Rothrock, R. A., Kaplan, J., & Van, D. O. (2018). The board's role in managing cybersecurity risks. *MIT Sloan Management Review, 59*(2), 12-15. Retrieved from https://sloanreview.mit.edu/

Roulston, K. (2018). Qualitative interviewing and epistemics. *Qualitative*

*Research,18(*3), 322-341. doi:10.1177/1468794117721738.

Safa, N. S., Maple, C., Watson, T., & Von Solms, R. (2018). Motivation and opportunity based model to reduce information security insider threats in organisations. *Journal of Information Security And Applications*, *40*, 247-257. doi:10.1016/j.jisa.2017.11.001.

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

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, *56*, 70–82. doi:10.1016/j.cose.2015.10.006

Sallos, M. K., & Garcia-Perez, A. (2019). Strategy and organizational cybersecurity: a knowledge-problem perspective. *Journal of Intellectual Capital*, *20*(4), 581-597. doi:10.1108/JIC-03-2019-0041.

Samhan, B. (2017). Can cyber risk management insurance mitigate healthcare providers intentions to resist electronic medical records? *International Journal of Healthcare Management. 13*(1), 12–21. doi:10.1080/20479700.2017.1412558.

Samtani, S., Chinn, R., Chen, H., & Nunamaker, J. F. (2017). Exploring emerging hacker assets and key hackers for proactive cyber threat intelligence. *Journal of Management Information Systems*, *34*(4), 1023-1053. doi:10.1080/07421222.2017.1394049

Santos, J., Palumbo, F., Molsen-David, E., Willke, R. J., Binder, L., Drummond, M., . . .

Thompson, D. (2017). ISPOR code of ethics 2017 (4th Edition). *Value in Health: The Journal of the International Society for Pharmacoeconomics and Outcomes Research*, *20*(10), 1227–1242. doi:10.1016/j.jval.2017.10.018.

Sawyer, B. D., & Hancock, P. A. (2018). Hacking the human: The prevalence paradox in cybersecurity. *Human Factors, 60*(5), 597-609. doi:10.1177/0018720818780472.

Schilke, O. (2018). A micro-institutional inquiry into resistance to environmental pressures. *Academy of Management Journal, 61*(4), 1431-1466. doi:10.5465/amj.2016.0762.

Scott, W. (1987). The adolescence of institutional theory. *Administrative Science Quarterly,* 32(4), 493-511. doi: 10.2307/2392880

Scott, W. R., & Amarante, J. M. (2016). Institutional theory's past and future contributions to organization studies. *Brazilian Administration Review*, *13,* 1-5. Retrieved from http://www.bar.anpad.org.br/

Setia, M. S. (2016). Methodology series module 5: Sampling strategies. *Indian Journal of Dermatology, 61*(5), 505-509. doi:10.4103/0019-5154.190118

Sharma, S. K., Al-Badi, A. H., Govindaluri, S. M., & Al-Kharusi, M. H. (2016). Predicting motivators of cloud computing adoption: A developing country perspective. *Computers in Human Behavior, 62*, 61-69. doi:10.1016/j.chb.2016.03.073

Shepherd, M. M., & Mejias, R. J. (2016). Nontechnical deterrence effects of mild and severe internet use policy reminders in reducing employee internet abuse. *International Journal of Human-Computer Interaction*, *32*(7), 557-567.

doi:10.1080/10447318.2016.1183862.

Sher, M. L., Talley, P. C., Yang, C. W., & Kuo, K. M. (2017). Compliance with electronic medical records privacy policy: An empirical investigation of hospital information technology staff. INQUIRY. *Journal of Health Care Organization, Provision, and Financing*, *54*(8), 1-12. doi:10.1177/0046958017711759

Sherer, S., Meyerhoefer, C., & Peng, L. (2016). Applying institutional theory to the adoption of electronic health records in the U.S. *Information & Management, 53*(5), 570-580. doi:10.1016/j.im.2016.01.002.

Shiau, W., & Chau, P. Y. (2016). Understanding behavioral intention to use a cloud computing classroom: A multiple model comparison approach. *Information & Management, 53,* 355-365. doi:10.1016/j.im.2015.10.004

Shires, J. (2018). Enacting expertise: Ritual and risk in cybersecurity. *Politics & Governance, 6,* 31-40. doi:10.17645/pag.v6i2.1329.

Singhal, N., & Bhola, P. (2017). Ethical practices in community-based research in nonsuicidal self-injury: A systematic review. *Asian Journal of Psychiatry, 30,* 127-134. doi:10.1016/j.ajp.2017.08.015.

Snelson, C. L. (2016). Qualitative and Mixed Methods Social Media Research: A Review of the literature. *International Journal Of Qualitative Methods, 15(*1), 1-15. doi:10.1177/1609406915624574.

Snyman, D. P., & Kruger, H. (2017). The application of behavioural thresholds to analyse collective behaviour in information security. *Information and Computer Security, 25*(2), 152-164. doi:10.1108/ICS-03-2017-0015.

Sohn, B. K., Thomas, S., Greenberg, K., & Pollio, H. R. (2017). Hearing the voices of students & teachers: A phenomenological approach to educational research. *Qualitative Research in Education*, *6*(2), 121-148. doi:10.17583/qre.2017.2374

Soilen, K. S. (2016). Economic and industrial espionage at the start of the 21st century–Status quaestionis. *Journal of Intelligence Studies in Business*, *6*(3), 51-64. doi:10.37380/jisib.v613.196

Sollars, M. (2016). Risk-based security: Staff can play the defining role in securing assets. *Network Security*, *2016*(9), 9-12. doi:10.1016/s1353-4858(16)30087-3.

Sommestad, T. (2018). Work-related groups and information security policy compliance. *Information and Computer Security*, *26*(5). 533-550. doi:10.1108/ICS-08-2017-0054

Sommestad, T., Karlzen, H., & Hallberg, J. (2015). The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Information and Computer Security*, *23*(2), 200-217. doi:10.1108/ICS-04- 2014-0025.

Sommestad, T., Karlzen, H., & Hallberg, J. (2019). The theory of planned behavior and information security policy compliance. *Journal of Computer Information Systems*, *59*(4), 344-353. doi:10.1080/08874417.2017.1368421.

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*, 215–236. doi:10.1016/j.ijinfomgt.2015.11.009.

Spiers, J., Morse, J. M., Olson, K., Mayan, M., & Barrett, M. (2018).

Reflection/commentary on a past article: Verification strategies for establishing reliability and validity in qualitative research. *International Journal of Qualitative Methods, 17*(1). doi:10.1177/1609406918788237.

Stanton, B., Theofanos, M. F., Prettyman, S. S., & Furman, S. (2016). Security fatigue. *IT Professional, 18*(5), 26-32. doi:10.1109/MITP.2016.84.

Steinbart, J., Raschke, L., Gal, G., & Dilla, N. (2016). SECURQUAL: an instrument for evaluating the effectiveness of enterprise information security programs. *Journal of Information Systems, 30*(1), 71. doi:10.2308/isys-51257.

Such, J. M., Gouglidis, A., Knowles, W., Misra, G., & Rashid, A. (2016). Information assurance techniques: Perceived cost effectiveness. *Computers & Security, 60*, 117-133. doi:10.1016/j.cose.2016.03.009.

Takahashi, A. R. W., & Sander, J. A. (2017). Combining institutional theory with resource-based theory to understand processes of organizational knowing and dynamic capabilities. *European Journal of Management Issues, 25*(1), 43-48. doi:10.15421/191707.

Tan, X., & Yu, F. (2018). Research and application of virtual user context information security strategy based on group intelligent computing. *Cognitive Systems Research, 52*, 629–639. doi:10.1016/j.cogsys.2018.08.016.

Tarlow, P. (2019). The human side of cybersecurity breaches. *International Journal of Safety & Security in Tourism/Hospitality, 20*, 1-4. Retrieved from https://www.palermo.edu/negocios/cbrs/ijssth.html

Thomas, L., & Briggs, P. (2016). Assessing the value of brief automated biographies.

*Personal and Ubiquitous Computing, 20(*1), 37-49. doi:10.1007/s00779-015-0896-2

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

Thornham, H., & Cruz, E. G. (2018). Not just a number? NEETs, data, and data logical systems. *Information, Communication & Society*, *21*(2), 306-321. doi:10.1080/1369118X.2017.1279204.

Tobin, M., Nugroho, D., & Lietz, P. (2016). Large-scale assessments of students' learning and education policy: Synthesising evidence across world regions. *Research Papers in Education, 31*(5), 578-594. doi:10.1080/02671522.2016.1225353.

Torraco, R. J. (2016). Writing integrative literature reviews. *Human Resource Development Review*, 15(4), 404–428. doi:10.1177/1534484316671606.

Torten, R., Reaiche, C., & Boyle, S. (2018). The impact of security awareness on information technology professionals' behavior. *Computers & Security, 79*, 68-79. doi:10.1016/j.cose.2018.08.007

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

perspective. *Computers & Security, 59*(1318885), 138-150. doi:10.1016/j.cose.2016.02.009

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

Tyler, J. (2016). Feature: Don't be your own worst enemy: protecting your organization from inside threats. *Computer Fraud & Security, 2016,* 19-20. doi:10.1016/S1361-3723(16)30063-X

U.S. Department of Health and Human Services. (1979). *The Belmont report*. Retrieved from http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html

Van Rijnsoever, F. J. (2017). (I Can't Get No) Saturation: A simulation and guidelines for sample sizes in qualitative research. *PLoS ONE, 12*(7), e0181689. doi:10.1371/journal.pone.0181689

Venkatesh, V., Brown, S., & Sullivan, Y. (2016). Guidelines for conducting mixed-methods research: An extension and illustration. *Journal of the Association for Information Systems, 17*(7), 435–494. doi:10.17705/1jais.00433

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2016). Unified theory of acceptance and use of technology: A synthesis and the road ahead. *Journal of the Association for Information Systems, 17*(5), 328-376. doi: 10.17705/1jais.00428

Visser, M. M., Van Biljon, J. A., & Herselman, M. (2017). Evidence-based case selection: An innovative knowledge management method to cluster public technical and vocational education and training colleges in South Africa. *South*

African Journal of Information Management, 19(1), 1-13. doi:10.4102/sajim.v19i1.751.

Vitak, J., Shilton, K., & Ashtorab, Z. (2016). 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). doi:10.1145/2818048.2820078.

Warkentin, M., Johnston, A. C., Shropshire, J., & Barnett, W. D. (2016). Continuance of protective security behavior: A longitudinal study. *Decision Support Systems*, *92*, 25-35, doi:10.1016/j.dss.2016.09.013.

Wheeler, A. J. A., & Mcelvaney, R. (2018). "Why will you want to do that work?" The positive impact on therapists of working with child victims of sexual abuse in Ireland: a thematic analysis. *Counselling Psychology Quarterly*, *31*(4), 513–527. doi:10.1080/09515070.2017.1336077.

Wilkin, C. L., Couchman, P. K., Sohal, A., & Zutshi, A. (2016). Exploring differences between smaller and large organizations' corporate governance of information technology. *International Journal of Accounting Information Systems*, *22*, 6-25. doi:10.1016/j.accinf.2016.07.002

Wirtz, B. W., & Weyerer, J. C. (2017). Cyberterrorism and cyber attacks in the public sector: How public administration copes with digital threats. *International Journal of Public Administration, 40*(13), 1085-1100. doi:10.1080/01900692.2016.1242614.

Wong-Riff, K. W. Y., Tsangaris, E., Goodacre, T., Forrest, C. R., Pusic, A. L., Cano, S.

J., & Klassen, A. F. (2017). International multiphase mixed methods study protocol to develop a cross-cultural patient-reported outcome instrument for children and young adults with cleft lip and/or palate. *BMJ Open, 7(1*), 1-9. doi:10.1136/bmjopen-2016-015467.

Yamin, M., & Sen, A. A. A. (2018). Improving privacy and security of user data in location-based services. *International Journal of Ambient Computing and Intelligence (IJACI), 9*(1), 19-42. doi:10.4018/IJACI.2018010102.

Yan, Z., Robertson, T., Yan, R., Park, S. Y., Bordoff, S., Chen, Q., & Sprissler, E. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment? *Computers in Human Behavior, 84*, 375–382. doi:10.1016/j.chb.2018.02.019

Yazdanmehr, A., & Wang, J. (2016). Employees' information security policy compliance: A norm activation perspective. *Decision Support Systems, 92,* 36-46. doi:10.1016/j.dss.2016.09.009.

Yin, R. K. (2016). *Qualitative Research from Start to Finish* (2nd Ed.). New York, NY: The Guided Press.

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). Los Angeles, CA: Sage.

Zafar, H., Ko, M. S., & Osei-Bryson, K. (2016). The value of the CIO in the top management team on performance in the case of information security breaches. *Information Systems Frontiers, 18*(6), 1205-1215. doi:10.1007/s10796-015-9562-5.

Zhang, K. (2018). Theory of planned behavior: Origins, development, and future Direction. *International Journal of Humanities and Social Science Invention, 7*(5), 76-83. Retrieved from https://theijhss.com/

Zhang, X., Kuchinke, L., Woud, M. L., Velten, J., & Margraf, J. (2017). Full length article: Survey method matters: Online/offline questionnaires and face-to-face or telephone interviews differ. *Computers in Human Behavio*r, *71*, 172-180. doi:10.1016/j.chb.2017.02.006.

Appendix A: Title of Appendix

Interviewee (Title): _____

Interviewer: _____

Interview Protocol:

_____ A: Demographics/ Interviewee Background

_____ B: Main Interview Questions

Other Topics Discussed: _____

Documents Obtained: _____

Post Interview Comments or Leads: _____

Introductory Protocol

In conducting the interview, I will like to record our interview. For your information and privacy, only the researcher of the project will have access to the tapes, and they will be gotten rid of eventually after the researcher is through with them. Importantly, this document states that: (1) all data will be held confidential, (2) your participation is voluntary, and you may withdraw any time if you wish to, and (3) we do not intend to inflict any harm. Thank you for your anticipated participation.

I have planned this interview to last no longer than 45 minutes. During this time, I will have several questions that I will like to cover. Please bear with me. The interview won't be longer than the planned time.

Interview Protocol

A. Demographics/ Interviewee Background

How long have you been

_____ in your present position?

_____ at this company?

B. Main Interview Questions

Post Interview Comments /Observations:

Appendix B: Interview Questions

Interview Questions

Demographic Questions

1. What is your current job role, and how many years have you spent on the job?
2. How many years of experience do you have in cybersecurity?
3. What other job roles have you held in the field of cybersecurity?

Interview Questions

1. What types of security programs do you manage?
2. What roles within your corporation assist in the development and implementation of security policies?
3. What methods do you utilize to enforce cybersecurity policies?
4. What prompted the need for the enforcement of cybersecurity policies?
5. What methods do you consider the best, and which approach do you consider least effective?
6. What factors influenced your decision to use the type of approach you use to implement cybersecurity policies?
7. What do you consider the merits of enforcing cybersecurity policies? What has been the impact on employee compliance?
8. What challenges do you face during cybersecurity policy implementation?
9. What internal threats and human factors affect enterprise information security and employee cybersecurity policy compliance in organizations?

10. What are the external threats that affect organizational information security?
11. In what ways and how often do you review the security architecture of your organization?
12. In what ways and how often do you review employee cybersecurity policy compliance?
13. What solutions do you use to overcome compliance challenges?
14. What solutions have you put in place to mitigate security threats?
15. What type of training programs does your firm organize for staff members to educate them on security, data privacy, and compliance?
16. What impact has the education had on the risk culture of your organization?
17. How do you stay abreast of emerging technologies and keep yourself updated in the continually evolving cybersecurity field to manage the security of your company's information assets, data, and resources?