2021

Cyberattacks Strategy for Nonprofit Organizations

Yawo Obimpe Kondo
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Yawo Obimpe Kondo

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

Review Committee
Dr. Gail Miles, Committee Chairperson, Information Technology Faculty
Dr. Gary Griffith, Committee Member, Information Technology Faculty
Dr. Bob Duhainy, University Reviewer, Information Technology Faculty

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

Walden University
2021

Abstract

Cyberattacks Strategy for Nonprofit Organizations

by

Yawo O. Kondo

MS, Walden University, 2018

MS, University of Maryland University College, 2011

BA, University of Nebraska at Omaha, 2006

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

2021

Abstract

Information system security managers (ISSM) in nonprofits face increased cyberattack cases because nonprofits often use basic technology to save on costs. Nonprofit owners and managers need solutions to secure their data from cyberattacks. Grounded in the general systems theory, the purpose of this qualitative multiple case study was to explore strategies ISSMs at nonprofit organizations employ to protect against cyberattacks. Participants included five IT managers and directors of information technology in charge of security management in nonprofit organizations in Maryland, the District of Columbia, and Virginia. Data was generated through interviews and reviews of archival documents. The data analysis technique used was thematic analysis. Three themes emerged from the analysis: cybersecurity awareness, cybersecurity strategy, and third-party dependence. The nonprofits should consider the following recommendations: first, evaluate cybersecurity health by assessing the existent cyber threat environment. Second, develop and execute a comprehensive strategic plan on cybersecurity, including policies and procedures targeted at protecting sensitive and likely sensitive data. Third, evaluate in-house IT capabilities and consider hiring third-party vendors with expert skills. Fourth, create cybersecurity awareness by training the employees on data protection. The implications for positive social change include the potential for ISSMs conveying effective cybersecurity strategies for nonprofits to mitigate and prevent potential cybersecurity attacks, thus furthering the nonprofits’ missions.

Cyberattacks Strategy for Nonprofit Organizations

by

Yawo O. Kondo

MS, Walden University, 2018

MS, University of Maryland University College, 2011

BA, University of Nebraska at Omaha, 2006

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

2021

Dedication

I wish to dedicate the research study to the Almighty God, who gave me the light and strength to conduct the research. I also dedicate my research to my parents Kondo Kokou Eloi and Allado Miekuna. Thank you, Mom, for endeavoring to show all of us the essence of struggle, integrity, and humility in every aspect of our lives. To my sister Kokoe, I love you more than you can think. To my late sister Enyonamvi, there is no day gone without me thinking about you since you passed on. To my children Lauren and Seyram dream and cultivate humility, be hungry for knowledge, trust your inner voice, and never give up even when things get difficult. Thank you, Cecilia, for being there when I was busy with the readings. To my siblings for always pushing me to be a better person.

Acknowledgments

I want to thank the committee members who have been instrumental in ensuring that I finish my project as desired. In particular, I thank Dr. Miles, whose works encouraged and guided me throughout this journey. I also thank Dr. Griffith and Dr. Duhainy, for the many suggestions throughout this study project. I am grateful to my relatives, Team Forever, Anna Williams, Affi, Kaagas, friends, and colleagues who throughout the study process provided me encouragement in each step of the DIT program. I am so grateful for your thoughts, prayers, and well wishes. Finally, thanks to the participants in this research to take time out of their busy schedules to meet with me and make the study a success.

Table of Contents

List of Tables

Section 1: Foundation of the Study

Background of the Problem

In the past, many considered cyberattacks as though it was a problem affecting for-profit organizations only. However, increased cyberattack cases among nonprofit organizations continue affecting their operations and even their existence (Carrapico & Farrand, 2017). According to Romanosky (2016), up to 3% of nonprofits report stolen or lost data cases. However, nonprofit companies encounter comparatively low litigation rates of 9% (Romanosky, 2016). Evidence from the study pointed out that while executives acknowledge cyberattacks' existence and express cybersecurity concerns, there is a significant gap between the worry and taking of action (Romanosky, 2016).

Several aspects of the operation of nonprofits expose their vulnerability to cyberattacks. For instance, nonprofits prefer bare-bones technology that may link to the desire to cut down on operational costs, such as using donated computers, old, unsupported software versions, and even outdated operating systems (Bauer et al., 2017). The earlier a system grows, the more it becomes susceptible to data breaches. Additionally, nonprofits commonly use open-source software as a means of saving on costs. The decision to use open-source software increases vulnerability to cyberattacks compared to using a proprietary version (Bauer et al., 2017). Many smaller nonprofits cannot maintain dedicated information technology (IT) staff for more lengthy periods. The lack of dedicated IT personnel exposes them to hackers who take advantage of the situation to breach their data (McMahon et al., 2015).

Problem Statement

Implementation of IT in nonprofits is a challenge that affects confidentiality, integrity, and privacy despite increasing cyberattacks (Garlinec et al., 2017). Data breach incident reports indicate a four-fold increase in the period between 2005 and 2014, from just slightly over 200 to over 1,200 incidents, meaning that cybersecurity incidents are on the rise for nonprofits (Romanosky, 2016). The general IT problem is that nonprofit organizations regularly face security risks. The specific IT problem is that some information system security managers (ISSMs) at nonprofit organizations lack strategies to protect against cyberattacks.

Purpose Statement

The purpose of this qualitative multiple case study was to explore the strategies that nonprofit organizations employ in protecting against cyberattacks. The specific population comprised IT managers and directors of IT in charge of security management in nonprofit organizations in Maryland, the District of Columbia, and Virginia. I conducted the study at different sites using participants' information. This study's social change implication is that people in charge of or engaged with nonprofits who may decrease identity theft and create safer environments. The impact of social change may be far-reaching because victims of cyberattacks suffer financial losses, operational disruptions, reputational damage, and legal ramifications, among other ill effects. With the pervasive nature of cyberattacks, many individuals suffer from stolen and misused data.

Nature of the Study

I selected the qualitative multiple case study for this research. A qualitative researcher uncovers and explores in-depth meanings and interpretations covering individual life experiences regarding a phenomenon (Daher et al., 2017). The qualitative method's suitability lies in its explorative potential for investigating technologies, practices, and policies used as part of the strategies by ISSMs at nonprofit organizations in protecting against cyberattacks. The quantitative method allows a researcher to examine the relationship between the independent variables and the dependent variable to explore and describe a situation (Grimaldo et al., 2018). I did not choose the quantitative method because I did not test hypotheses or the theories or review statistics. Using a mixed methods approach would have required coupling the qualitative and quantitative methodologies, which would have included testing hypotheses (Snelson, 2016). Because I did not test hypotheses, I considered the mixed methods approach inappropriate for my study.

A case study design focuses on undertaking in-depth learning of a given situation to narrow down a broad research field to establish an easily researchable topic (Margaret, 2016). I chose a multiple case study to examine several cases to understand the similarities and differences of IT security strategies in nonprofit organizations. Other options included the ethnographic design, which is based on a thorough study and explanation of a particular place and its culture, people, social structure, and behaviors (Bamkin et al., 2016). I did not choose the ethnographic design because my goal was not to conduct a cultural study. The phenomenological model mainly determines a lived experience based on a philosophy (Mayoh & Onwuegbuzie, 2015). I did not choose phenomenological design because my focus was not on understanding of a unique lived experience.

A case study constitutes an empirical inquiry into a contemporary phenomenon that happens in a real-world context, mainly where the distinction between context and the phenomenon is unclear (Yin, 2017). Adopting the case study research design requires the impartial collection of data from real-life situations and the determination of answers about the how, the what, and the why of the data (Yin, 2017).

Research Question

RQ: What are the strategies that ISSMs at nonprofit organizations employ to protect against cyberattacks?

Interview/Survey Questions

1. How do you evaluate data breaches in your organization regarding whether the organization is succeeding in containing them or they are spiraling out of control?
2. Between internal and external data breaches, which ones affect your organization the most, and why?
3. Which strategies do you use to ensure your IT staff are qualified to address security breaches? Why or why not?
4. Which strategies do you employ to ensure your IT department has an adequate budgets to address data breaches? Why or why not?

5. Does your organization create security awareness for employees through special programs implemented by the IS manager?
6. What procedures does your organization implement to conduct internal compliance audits as part of the strategies used to protect information from cyberattacks?
7. What data safety processes does your organization implement to guard against unauthorized access to the organization’s networks?
8. How often does your organization train its staff about the best practices for IT security? Do you think this is enough, and why or why not?
9. What is the extent of process automation in your organization regarding strategies used to protect information from cyberattacks?
10. How often does your organization periodically discard personal information at their disposal that is no longer required as part of a strategy to protect information from cyberattacks?
11. What are the procedures adopted by your organization in discarding personal information that is no longer required in protecting information against cyberattacks?
12. Which strategies do you feel your organization should adopt to enhance IT security?

Conceptual Framework

I used a general system theory (GST) for my conceptual framework. Von Bertalanffy authored GST in 1968, and its premises were that complex systems share the same organizing principles that can be determined and modeled mathematically (Kristof et al., 2019). It is a general theory that consists of systems science, systems technology, and systems philosophy (Verhoeff et al., 2018). The main philosophy of the GST is based on how the system works together and how one part of the system leads to understanding the other parts. Chen et al. (2012) described this level of cooperative interactions and ongoing relationships within the system as holistic. Rousseau et al. (2018) further described the general system as a complete system or natural organism stage with no alteration.

While advancements in technology have contributed to new business innovations, they also pose threats to organizations regarding the increased possibility of losing their valuable information. These challenges need holistic approaches that encompass collaboration and interrelationship to meet the security objectives (von Bertalanffy, 1972). In this study, the GST application consisted of using the various subsystems (input) to produce a secure outcome (output). Cyberattacks increase when there is no harmony between the policies, software, hardware, and training. Applying the von Bertalanffy GST approach to the study helped me assess how the subsystems work with each other.

Definition of Terms

Cloud: A computational paradigm comprising five critical characteristics of self-service on-demand, resource pool, broad network access, rapid elasticity, and measurable services. Cloud computing also exists in three different service models: platform as a service, software as a service, and infrastructure as a service (Marchisotti et al., 2019).

Cyberattack: Digital data damages and breaches attributed to illegal exploitation and application of confidential and personal information (Meisner, 2018).

Cybersecurity: A policy area that focuses on managing cyber threats, including disruption, unauthorized access, and alteration of electronically stored information, hardware, software, networks, and services (Yost, 2016).

Data breach: Situations where external parties get access without authority to a large volume of confidential customer data, such as credit card, address information, and so forth. The unauthorized access often results from individuals either within or outside the firm that seeks to exploit insecure or erroneous software, tamper with or pilfer hardware, and introduce malware to the systems (Kude et al., 2017).

Encryption: A mechanism used for intentionally masking data from unauthorized persons who may use it in unintended ways and cause security issues. Encryption obscures data using specific algorithms (El-Bendary, 2017).

Firewall: Vital hardware or software used between two or more networks that apply access control. A firewall guarantees security in the network as it sieves through all incoming and outgoing data to ensure that only relevant and secure data is allowed through (Alabady et al., 2018).

Malware: An abbreviation for malicious software. Malicious software targets computers and computer users by corrupting files, stealing information, or just introducing mischievous activities that annoy users (Tahir, 2018).

Assumptions, Limitations, and Delimitations

Assumptions

According to Wolgemuth et al. (2017), research assumptions constitute ideas that a researcher accepts as accurate even though that same position may lack factual backing. As the researcher for this doctoral study, I had the following assumptions. I assumed the review of documents from nonprofits and the interviews with organizational managers from the nonprofits provided adequate data for answering the research question. I assumed the research participants offered honest answers that would help in enhancing the validity of the study.

Limitations

Research limitations of any particular study refer to the potential weaknesses beyond the researcher's control and closely associate with the research design, funding constraints, statistical model constraints, and other factors (Theofanidis & Fountouki, 2019). The number of participants I interviewed depended on the number of nonprofits available in Maryland, the District of Columbia, and Virginia. Moreover, organizational policy regarding the release of information considered internal and private limited my access to data that could have been relevant.

Delimitations

Research delimitations constitute the definitions the researcher chooses to set, signaling the limits or boundaries of their work such that the objectives and aims of the study become practically achievable (Theofanidis & Fountouki, 2019). Unlike limitations that fall outside the researcher’s control, with delimitations, the researcher is entirely in control (Korrapati, 2016). Delimiting factors include the research questions, the choice of objectives, theoretical perspectives adopted, the study population, and variables of interest (Wolgemuth et al., 2017). The quality of any research reflects the ability of the researcher to deal with personal biases effectively. High quality will help in presenting objective research data (Wolgemuth et al., 2017). The delimitation of this study was that it entailed nonprofit organizations with the following characteristics: (a) organizations licensed to operate legally in the state of Maryland and the District of Columbia; (b) organizations with at least 150 personnel; (c) organizations that implemented cybersecurity measures effectively, and (d) organizations with at least $5 million in annual gross revenue. Nonprofits that did not meet the above criteria did not participate in the study.

Significance of the Study

The purpose of this study was to explore strategies some ISSMs at nonprofit organizations use to protect against cyberattacks. The research findings could help IT managers and directors of IT protect their organizations against cybersecurity threats. To the IT organizations, the study could provide insight that they can use to enhance cybersecurity in their premises and help guarantee customer trust. This study could be useful for chief information officers (CIOs) and chief information security officers (CISOs) to develop the strategies they need to protect their information. The findings could also help the IT managers and directors of IT develop a plan of action to mitigate cyber threats' effect on their performance.

Additionally, the information could help IT managers develop internal cybersecurity training to improve the data security in the organization. Nonprofit organizations inadvertently expose their assets to security breaches, as do for-profit organizations. Cyber threats can affect an organization's productivity and finance. Through this study's findings, IT practitioners may have tools for developing effective cybersecurity strategies to safeguard data in nonprofit organizations. The employees may participate in cyberthreat literacy campaigns where they transfer their knowledge to the community members. Such experience may result in a general understanding of cyber threats and, as such, a safer community as far as cybersecurity is concerned.

In terms of social change, Bach-Mortensen and Montgomery (2018) observed that nonprofits occupy a critical position in society because they provide valuable services or products to the community, targeting such vulnerable groups as the elderly, people with disabilities, children, and at-risk young people. According to the National Council of Nonprofits (2016), nonprofits provide essential social services, such as shelter, food, and emergency response, benefiting millions of Americans. In this study I sought to highlight critical cybersecurity strategies that may help executives in nonprofits ensure their systems and internal documents are safe from hackers. With the enhanced system safety, the nonprofits could safeguard data about their beneficiaries, including the elderly, people with disabilities, children, and young people, thus protecting their privacy.

A Review of the Professional and Academic Literature

A literature review is a critical aspect of any research as the researcher uses it to build on previous studies and the available knowledge base to inform the latest research

(Boell & Cecez-kecmanovic, 2015). This research's focus required studying cyberattack strategies effectively employed by nonprofit organizations to keep their data safe. I used the literature review to further this objective by providing factual details on the topic of interest as reported by researchers who have studied and conducted research in this area. The conceptual framework I chose for the study was the determinant of the choice of literature sources. The GST, which von Bertalanffy authored in 1968, was the study's foundation. Literature sources reviewed in this study explored GST topics and alternative theories that compared or contrasted with them.

For this research I drew from various resources, including IEEE Source Library, ProQuest, EBSCOhost, Google Scholar, government websites, and Science Direct. I knitted the research topic, which was IT security strategies used to protect information from cyberattacks to nonprofit organizations, using such search terms as *IT security strategies against cyberattacks in nonprofits, cyberattack security strategies in American nonprofits,* and *information protection strategies in nonprofits.* Given that IT is a fast-growing area of academia, older literature materials tend to lose relevance with time. Thus, I focused this literature review on more recent sources published between 2015 and 2020. I gathered 165 different sources for the literature review, 98% of which were peer-reviewed articles. Up to 96% of the 165 sources were published in 2015 or later. Overall, the literature review offers a critical analysis of the topical issue determined by the research question. The literature review is structured into four main areas to enable logical discussion. These four sections include the conceptual framework, which provides a full explanation of the original GST theory and its evolution, supporting and contrasting approaches, and other studies that align with the various methods. The literature review sections address data breach, data governance, security, and privacy.

General System Theory

Von Bertalanffy introduced the GST in 1968; in it he described the world as based on irreducibly integrated systems. His discovery offered a framework on which to ground the core aspects of disciplines and issues in a systematic and reasoned corpus of knowledge (Drack & Pouvreau, 2015). In the past, science focused on explaining observable phenomena by breaking them down to an interaction between elementary units capable of being investigated separately (Bertalanffy, 1968). According to Bertalanffy (1968), this focus differs from contemporary science concepts, which are more about “wholeness,” which is somewhat vague. Modern science therefore focuses on problems of organization, dynamic interactions visible in the disparity of behavior of parts existing in isolation or a higher arrangement, and so forth. Conceptions and issues of this nature are common in all science branches, whether inanimate things, social phenomena, or living organisms are the object of study (Bertalanffy, 1968).

The GST is used to identify the wholeness or entirety of scientific and social problems (Bridgen, 2017). The underlying aim for applying the GST is to attain a metascientific framework through general systemology, which resulted in much-needed incorporation into scientific education (Drack & Pouvreau, 2015). Such an exact approach is crucial in the nonphysical areas of science. This theory is closer to the unity of science's objective, as it develops on principles running “vertically” throughout the universe of the separate sciences (Bertalanffy, 1968). Essentially, the GST concept aligned with this study's purpose because cyberattacks constitute scientific and social problems afflicting nonprofit organizations across the United States. The exploration of strategies used by ISSMs at nonprofit organizations to protect against cyberattacks attains a meta scientific framework through general systemology.

According to Schneider et al. (2016), GST is a more focused way of thinking that takes a world view as its proportion. As an open system, the organization persistently interacts with its local environment by exchanging “materials” (Schneider et al., 2016). Additionally, the organization also interacts with the external environment elements (Turner & Baker, 2019). Although each of these social systems bears distinct nonmaterial characteristics, they all match the basic makeup of living open systems. GST is more involved with the uniformities contributing to their processes and functioning principles than their structural similarities (Kordova et al., 2018). As Schneider et al. (2016) explained, GST is used to seek fundamental concepts with greater relevance to all systems.

The significance of GST as the foundational theory of this research lies in the fact that many nonprofit organizations have integrated their operations in computers and computer systems. There is a possibility that these charitable organizations' activities will stop when malicious people hack computers and computer networks. This threat faces virtually all organizations that rely heavily on computerized processes (Posey et al., 2017). The reality of this threat often results from the fact that many nonprofit organizations only invest in basic computer systems easily intruded upon for their operations to be affected by hackers. In such instances, the nonprofit organizations end up losing crucial data. Nonetheless, the GST concept can help change the norm in how nonprofit organizations operate by specifically proposing better organizational systems that enhance efficiency. The GST foundational theory suggests superior systems that will prove challenging to be manipulated easily by hackers that would result in service disorientation.

Evolution of the General System Theory

Several scholars have continued looking at von Bertalanffy's GST theory with a view of expanding it to create more elaborate meaning. As GST evolved, researchers transformed the method into an interdisciplinary study field involving different concepts, principles, and models. New theoretical systems approach, such as cybernetics, control theory, the theory of automata, information theory, relational mathematics, set, graph, and network theory, computerization and simulation, and game and decision theory all fall outside GST (Von Bertalanffy, 1972). Nonetheless, GST and systems theory are considered the fields' standard for several other social science disciplines. These numerous theoretical systems approaches, according to Von Bertalanffy (1972), tie to systems problems.

Examining the progress of systems theory over time shows a variety of intellectual activity and a practical endeavor. The first peculiarity of the general field of work about systems theory lies in expanding systems ideas for itself (such as cybernetics) and applying systems ideas in a given discipline (Krippner et al., 1985). In the branch that focuses on work within the systems sciences, a distinction exists between the purely hypothetical advancement of systems ideas and their interrelationship and effort to develop systems ideas considered significant in interpreting or handling real-world conditions (Moore et al., 2017). Still, other examples lead to a threefold distinction, including rigid systems approaches (for instance, those employed in systems engineering), soft systems approaches (for example, those adopted in humanistic psychology), as well as hybrid systems approaches (for example, those used in operations research for aiding decision-making).

According to Muegge and Craigen (2015), the general systems theory offers a significant basis for effectively addressing cybersecurity. Employing Muegge and Craigen's argument, Ogliastri et al. (2016) supported their views by demonstrating the GST approach's applicability in the case of nonprofits and their management of data to prevent breaches. Reviewing some of the effective strategies employed by nonprofits towards protection against cyberattacks may offer the best practices, enhance consumer confidence, and inspire economic prosperity (Ogliastri et al., 2016). These strategies provided the foundation of this study to explore the IT security strategies used to protect information from cyberattacks on nonprofit organizations.

Supporting Theories

According to Horne et al. (2016), there is no apparent information security theory. Stronger theory, as Horne et al. (2016) further argued, can be achieved by linking theories of varied types. Horne et al. (2016) agreed that there are several theories related to information security, such as theory of information warfare (TIW) and theory of Protection Motivation (TPM), but they noted that none of these theories have their focus of knowledge anchored in information security alone. Managing cybersecurity risk also raises the probability of an organization meeting its objectives by maximizing the opportunities that may come up (Garlinec et al., 2017).

Theory of Information Warfare

The TIW, compared to GST, is a relatively new framework with its origin attributed to Sun Tzu (512 BCE), following the vast leap in communication technologies as well as the internet (Baskerville, 2010). Communication and technological advancement resulted in strategic consequences affecting governments, armed forces, and the general population (Monov & Karev, 2018). Today, multiple names used for information warfare represent many dimensions and various purposes. According to Libicki (2017a), in the context of modern technologies, TIW includes sophisticated means of messaging, representing some level of limited war carrying a low level of escalation while providing opportunities for geopolitical advancement goals at minimal cost. Libicki (2017a) found that information warfare falls under a type of transnational threat, mainly affecting national security, penetrating national borders and weakening stability. Monov and Karev (2018) emphasized that TIW is more about the influence over leaders and the population and control over actions and decisions. Given the above analysis, TIW was not an appropriate framework for the cyberattacks strategy for nonprofits. This theory is mainly relevant where national security aspects affecting governments and armed forces are involved.

The Protective Management Theory

The protective management theory (PMT), on the other hand, focuses on the extent of severity of harmful events, perceived susceptibility to the threat (such as the probability of its occurrence), concern regarding the risk, and the availability and efficiency of a coping response to lessen or eradicate the potential harmful event (Clubb & Hinkle, 2015). Rogers (1975) was the original PMT theorist, and the underlying assumption of his theory is that fear appeals could cause attitudinal changes. PMT's purpose was to do away with response patterns capable of producing harmful consequences or creating models of response that might thwart the occurrence of deleterious events (Rogers, 1975). Individual cognitive processes influence the resultant effects of such support or deterrence factors. PMT and GST have similarities in the sense that both are social theories. This similarity means that they offer ideas, arguments, hypotheses, explanatory speculations, and thought experiments regarding human societies and elements or structures making up such societies. In recent studies undertaken by Wong et al. (2016) on the PMT concept, the outstanding view was that both individual and environmental factors can offer either support or deterrence to practicing protective behaviors. Rajendran et al. (2017) notably confirmed PMT's widespread application in information systems security policy. For instance, they mention a proposal model that offers explanations about employees' security compliance. This model is useful for cybersecurity, especially as it would enable employees in organizations, such as nonprofits, to adhere to a set of behaviors that would deter them from aiding data breaches in the organization (Rajendran et al., 2017). Although PMT has been applied mainly in information systems security policy, I did not choose the theory for this study because it focuses more on the aftermath of the challenge. It concerns the extent of the severity of harmful events, perceived susceptibility to the threat, and concerns regarding the risk. This focus is not consistent with this study's objective, which was to explore the cyberattacks strategy for nonprofit organizations to keep data safe from hackers.

The Principles of the Theory of Protection Motivation

The principles of the TPM use a social perspective to devise strategies that organizations such as nonprofits can rely on to establish adequate protection against cyberattacks (Sommestad et al., 2015). According to Barlette et al. (2017), TPM can effectively predict an individual's willingness to employ protective behaviors as far as cybersecurity application is concerned. Barlette et al. argued that using the TPM could help test factors explaining the behavioral intentions and the actual behavior of managers in organizations, such as nonprofits, in engaging in defensive information security measures. Doherty and Tajuddin (2018) agreed with Barlette et al.'s observations, noting that practitioners and managers can deal with cybersecurity challenges by encouraging colleagues to identify and consider their information as a precious resource. This approach will enable the nonprofits to improve their conformity to information security protocols (Doherty, & Tajuddin, 2018).

Comparatively, the GST approaches the cybersecurity strategy discourse from a systems integration point of view, where the organization must have a mix of strategies to guarantee data security (Kordova et al., 2018). Doherty and Tajuddin (2018) viewed the general systems approach towards securing organizational data as preferable to persuasion of employees to observe information security policies and educating them on the significance of their handling of information. According to Doherty and Tajuddin (2018), nonprofits can train their employees to enhance their willingness to take the necessary steps to protect data. Kim and Kim (2017) argued that if nonprofits wish to achieve the highest level of compliance behavior among their employees, there needs to be a material culture and infrastructure supporting compliance. Nonprofits must also promote compliance systems in general to encourage the employees to put in voluntary efforts.

Another supporting theory to the GST and its application is the cybernetic or control theory. This theory constitutes a general approach to understanding self-regulating systems (Theophanidis et al., 2017). Nikolić (2015) explained that the cybernetic or control theory's central ideas date back to 1929 during the discussion of homeostatic physiological mechanisms. However, Mowlana (2019) elaborated that the birth of the theory as a separate body of thought links to the book *Cybernetics: Control and Communication in the Animal and the Machine* by Wierner in 1948. Proctor and Xiong (2018) argued that cybernetics set the stage through the idea that everything beginning from neurophysiological systems to societal activities can be made into structured control systems constituting feedforward and feedback loops. Proctor and Xiong further found that information theory provided a way through which entropy and information can be quantified and upheld theorizing through information flow. Proctor and Xiong also highlighted that statistical theory presented a means for arriving at scientific inferences drawn from the findings of controlled experiments and abstracting human decision making. These three pillars marked cognitive psychology's evolution in the information age (Proctor & Xiong, 2018). Advancement in technology in the information age has caused increased intertwining of human lives with the cyber environment. This intertwining has, in turn, made cognitive psychology a critical aspect of interdisciplinary research as far as the intertwining is concerned (Proctor & Xiong, 2018). Nonetheless, I did not adopt this theory for this study because it focuses more on the organization's psychological aspect instead of an overall approach that I sought to achieve with this research.

According to Mingers and Standing (2018), cybernetics or control theory employs simple mathematical ideas to institute a fundamental framework for discussing feedback, equilibrium, stability, disturbance, information, entropy, regulation, noise, constraints, and transmission (communication). When looked at from a cybernetics perspective, the system theory provides the tools that focus on taking on the cyber cycle (De Boer & Andersen, 2016). De Boer and Andersen's (2016) views coincided with Fal's (2016) observation describing the cybernetics as closed-loop feedback mechanisms with output that links directly with the subsequent system's input. According to Drack and Pouvreau (2015), the feedback loops and the other communication channels making up the systems may utilize behavioral relations instead of physical connectivity. Drack and Pouvreau's description captures Hof's (2018) elaboration of the cybernetic perspective's central concept in terms of actions by the attacker or defender impacting the rival system's input. In this dissertation, however, the main focus was not on the functioning of feedback mechanisms from external environments to the organization and how they relate to cyberattack strategies. Instead, the focus was on how, as an open system, the organization persistently interacts with its local environment by exchanging 'materials' and how it relates to cybersecurity. GST theory captures the best explanation of this situation, looking at the organization as an open system that interacts with the external environment.

Cybernetic concept's application in an organization's scenario taking on data security challenges implies that an attacker will make use of the organization's output to change their output and negatively affect the operations (Pillay, 2017). According to Pillay (2017), the attack could be of any type, including intrusion or denial-of-service, which would either way still end up causing some level of disturbance input to the organization's system. Horvath and Lovasz (2018) agreed with Pillay (2017), noting the defender's expectation of detecting the disturbances within the organization's system and attempting to alleviate those inputs using such methods as adding firewalls to control network access, resetting their systems, or developing patches. The cycle will continue indefinitely, provided the defender only acts in response to recognized/detected input disturbances (Horvath & Lovasz, 2018). As a theory, cybernetics proposes a control structure that aids decision making within the system (Xu et al., 2016). The primary control cycle constitutes a receptor (sensor or detector) that registers various stimuli (Xu et al., 2016). Through the monitoring and response feedback mechanism, the system can achieve self-regulation (Fal', 2017). According to Fal' (2017), the self-regulation would apply effectively in organizational set-up in detecting cyberattacks and providing feedback to trigger self-regulation.

Contrasting Theories

GST's principal view of the organization as being in constant interaction with its local environment through the exchange of 'materials' counters the position assumed by the TPM. According to the TPM, an individual's willingness to employ protective behaviors is enough to take on cybersecurity challenges (Schneider et al., 2016). According to Kordova et al. (2018), GST's guidelines concern more the uniformities contributing to organizations' principles of processes and functioning than their structural similarities. Therefore, the use of GST principles proposes better organizational systems that enhance efficiency in data protection and management in nonprofits (Posey et al., 2017).

The Complex Adaptive System

The complex adaptive system (CAS) theory has different principles to those of the GST. In particular, CAS has its laws premised on open dynamical systems capable of self-organizing their structural configuration using information exchange, energy, in addition to other resources found in their environment (Coetzee et al., 2016). The systems are capable of changing these resources to support action, and their self-organizing nature has little or absolutely no direct influence on these systems from outside forces (Junior, 2016). The CAS's founding was in 1987 at the Santa Fe Institute (SFI), during the SFI meeting that was discussing complexity in economics (Citera, 2017). Several theorists are behind CAS, including physicists, economists, and so forth. One of the most renowned theorists behind the CAS was John Henry Holland, who conceptualized a genetic evolution 'adaptive plan,' which progressively modified structures using suitable operators (Citera, 2017). Mittal et al. (2017) recorded that Holland's adaptive plans created interest in methods of programming computers to achieve problem-solving capabilities.

The fundamental tenets of CAS include non-linear dynamics, adaptation/evolution, chaos theory, self-organization, feedback, and chaos (Preiser et al., 2018). Thus, the CAS perspective considers systems based on non-linearity, implying that future states are irregular (Preiser et al., 2018). According to Preiser et al., transitioning a system from simple to complex nature results in reduced predictive mechanisms' reliability. Chaos is deterministic and equally linear, and with mathematical meaning, sensitive to its initial circumstances (Junior, 2016). CAS involves linear and predictable mathematical modeling when viewing chaos (Turner & Baker, 2019). The use of mathematical modeling guides chaos into identifying global patterns based on the components' interactions in as far as self-organizing systems are involved. According to Shapiro (2015), emergence is a significant element of CAS as it happens when the system components' interaction results in new states that contribute to the system's unpredictability. The other tenets of feedback, evolution, and adaptation refer to a system's ability to learn, all of which exist in chaos and CAS (Werder & Maedche, 2018).

CAS contrasts with GST on account of an open and closed system (Shapiro, 2015). According to Shapiro, the theoretical methods approach generally aligns with closed systems, although this may not always be. Hodiamont et al. (2019) agreed with Shapiro, noting how several GST approaches look at open systems, particularly those concentrating on social networks. Hodiamont et al., however, point out that CAS predominantly associates with open systems. CAS is portrayed as unordered, complex, and chaotic system in which patterns can surface (open system: Reiser et al., 2018).

Contrastingly, Schneider et al. (2016) noted GST's association with order arrangement and practice in the sense that there are complicated and straightforward structured patterns (closed system). The main difference between an open and a closed system exists in the second law of thermodynamics that applies majorly to closed order (MacDougall, 2019). The second law of thermodynamics relates to theoretical systems approaches (MacDougall, 2019). CAS contrasts the second law of thermodynamics because of the doctrine of self-organization and emergence (Adauto & Guerrini, 2018).

The CAS theory is relevant, particularly about cybersecurity in nonprofits, because it recognizes the highly complex problems that have emerged due to the continued use of IT in organizations. CAS theory, thus, advocates for a new approach to tackle the complex decision spaces that organizations have become (Coetzee et al., 2016). According to Törmänen et al. (2016), CAS principles facilitated intelligent adaptive kind of systemic behavioral responses to address the complexity. As nonprofits deal with the severe challenge of data loss and cyber insecurity, the CAS approach advocates systems of systems intended to create intentionally designed and preferred emergent behavior utilizing self-organized intelligent, and focused constituent systems (Coetzee et al., 2016). The choice of GST over CAS for this dissertation follows the realization that CAS is predominantly unordered, complex, and chaotic in which patterns can surface (open system; Preiser et al., 2018). This complexity would make it difficult to work with when trying to adopt it as the basis of explaining cyberattack strategies for nonprofits. Unlike CAS, however, GST has good order. There are complicated and straightforward structured patterns (closed system; Schneider et al., 2015), making it easy to work with when adopting the concept to explain cyberattack strategies for nonprofits.

Vulnerabilities of Nonprofits Computer Systems

For-profit organizations dedicate much time and resources towards enhancing their data security, while nonprofits usually adopt inferior policies against data protection and management (Gordon et al., 2015). For instance, in line with Gordon et al.'s observation, many types of research have revealed the misconception among nonprofit managers that their organizations are not as highly at risk to hackers as are for-profits. However, as the latest data breaches have demonstrated, nonprofits are just as targeted by hackers as for-profit organizations (Bordoff et al., 2017). Nonprofits often have constricted budgets that are mostly unable to fund effective IT and control assessment capable of offering better protection (Gordon et al., 2015).

In many cases, nonprofits lack staff in their IT departments with the necessary skills to provide some cybersecurity specialty functions (Jalali & Kaiser, 2018). According to Gordon et al. (2015), the main reason for this occurrence is that nonprofits' primary objective is to serve specific goals, work towards a mission, and focus efforts towards getting funding and cutting their costs. The ownership of nonprofits, including the management and staff, all focus on fulfilling these goals. Their entire incentive structure defines their working towards achieving these objectives. Jagalur et al. (2018); nonetheless, these goals are not in tandem with good cybersecurity in general. Moreover, nonprofits' employees often thought that cybersecurity is less critical because they do not consider their organizations a valuable target for cyber-crime (Almubark et al., 2016). While there is no guarantee that a cybersecurity strategy and regular security assessments will prevent dangerous threats, the truth is that the nonprofits increase their chances of limiting exposure with an approach. Such a strategy equips the nonprofits to plan, review, test, and evaluate their weaknesses ahead of the attacks (Almubark et al., 2016).

Data Breach

A data breach is a severe concern that virtually all organizations think about because of the potential damages it leaves in its wake. Prakash and Singaravel (2015) described data breaches as organized actions to extract hidden knowledge from people's data collections without the people authorizing it. In their view, Prakash and Singaravel noted that organizations storing extensive data about people may decide to mine this data for purposes of learning other individual trends about the people, including their preferences, models, patterns, and so forth. The issue of a data breach is not only confined to for-profit organizations but also affects nonprofit organizations a great deal (Levesque et al.,2015). Holtfreter and Harrington (2015) cited a case that happened in May 2006. A fraudulent Red Cross employee interfered with the database and accessed up to a million records, some of which included donor social security numbers. This incident at the American Red Cross fits Sen and Borle's (2015) description of a data breach as an incident where unpermitted access to sensitive, confidential, or protected data happens. When this unauthorized access occurs, there is a higher likelihood of compromising integrity, confidentiality, and availability of the same data in question (Sen & Borle, 2015). While there is detailed documentation of data breaches in for-profit organizations, with substantial efforts to address the menace, the same cannot be said for the nonprofit organizations because of several challenges (Gordon et al., 2015).

Often, nonprofit organizations lack adequate funding to develop IT and control assessment units that can work towards achieving better protection (Mierzwa & Scott, 2017). Echoing Mierzwa and Scott's assertions, Jagalur et al. (2018) found that nonprofit organizations often lack staff with cybersecurity specialties to take charge of their IT unit. According to Mierzwa and Scott, nonprofit organizations lack adequate budgets and personalities for their IT departments because their primary objective is to serve specific goals, endeavor to achieve a mission, and concentrate more on acquiring funding and cutting costs. In their estimation, they consider these nonprofit organizations' goals as not aligning with good cybersecurity. A perfect example that highlights Mierzwa and Scott's arguments reflects big charity organizations such as The Red Cross. In many instances, the Red Cross uses individuals as volunteers to achieve their objectives (International Federation of Red Cross and Red Crescent Societies, 2019). However, the idea of working with volunteers means that the organization may not get the most qualified individuals to serve in their departments, especially for such highly demanding departments like IT. The lack of competitive salaries arguably makes it difficult for nonprofits to attract the best IT skills, leaving most of them at the mercy of less skilled volunteers (Jagalur et al., 2018). Aranda et al. (2018) observed that unlike employed workers, volunteers increase the risk of data breaches because they may not be as committed to their social contract as would permanently employed staff. However, with the ever rising threat of data breaches, nonprofit organizations have embarked on various strategies to protect themselves from the risk (Holtfreter & Harrington, 2015).

Nonprofit Strategies to Secure Data

Many nonprofit organizations are putting in place strategies to combat data breaches on their premises. According to Bauer et al. (2017), one such approach includes creating awareness about information systems through special programs implemented by IS managers. These programs entail systematically planned interventions that continuously convey security information to the targeted audience (Bauer et al., 2017). Almubark et al., (2016) observations are in tandem with Bauer et al., who indicated that the best way nonprofits can motivate employee behavior to curb data breaches is by creating an influential security culture. This strategy works because creating an influential security culture keeps the employees updated about the technology, including enabling them to understand the processes and other organizational factors that touch on data security (Almubark et al., 2016). Considering the same argument as Almubark et al., Zafar et al. (2016) insist that having an influential culture about data security is enhanced through awareness training, risk management activities, and security planning activities. In modern organizations, Zafar et al. observed that the top management's support for IT governance practices entailed internal conduction of compliance audits, establishment of data classification frameworks, offering a data governance team, and having the position of a chief security officer. As identified by Zafar et al., this arrangement can be replicated in nonprofit organizations in a bid to control instances of breach of data.

Apart from creating cybersecurity awareness in the organization, authentication equally constitutes a strategy against nonprofit organizations' data breaches. Authentication entails a process for ascertaining accurate and authentic claims on a particular subject or regarding a matter (Mohammed et al., 2017). In nonprofits, instituting authentication as a data safety process would guard against unauthorized access to the organization’s networks, in addition to protecting users’ identities and guaranteeing the true identity of the user (Bidgoli, 2018). In particular, Reddy et al. (2016) explained that most cryptographic protocols entail some endpoint for authentication seeking to thwart man-in-the-middle (MITM) attacks specifically. A perfect illustration of this framework that nonprofits can consider for the safety of their data includes the 11 Transport Layer Security (TLS) or the Secure Sockets Layer (SSL; Liu et al., 2018). Both TLS and SSL work by continuously encrypting network connection segments at the Transport Layer (Liu et al., 2018). Bharathi (2017) explained that data are brokering, exposure of personal data globally, and the deficiency of governance-based security design form part of the leading security issues that organizations are grappling with currently. Nonprofit organizations can rely on SSL or TLS to verify the server via a jointly trusted certification authority (Liu et al., 2018). Moreover, Pascalev (2017) mentions the possibility of nonprofit organizations using the Bull Eye algorithm to observe all sensitive information from a 360° perspective. When nonprofit organizations use this algorithm for their data security, they will manage relations involving replicated data and original data (Pascalev, 2017).

Three hundred sixty-degree security is yet another strategy available to nonprofits in their efforts to deal with the data breach menace (Kholidy et al., 2016). The 360-degree security strategy, as Kholidy et al. elaborated, is a plan for responding in depth to the security measures of the nonprofit organization. Agreeing with Kholidy et al., Woszczynski and Green (2017) found the first step of implementing the 360-degree security strategy was identifying assets of value to ensure their shielding from potential risks that could result in data breaches. After identifying value assets, the purpose is to ensure that they are all under the right controls (Woszczynski & Green, 2017). However, just ensuring that the assets are under the proper controls is not enough. Moskal et al. (2018) insisted that the nonprofit organization's protection of valuable assets ought to be verified throughout by way of proper testing and simulation. There must be an existing process that guides the improvement and governance procedures to provide ongoing confidence within the controls (Moskal et al., 2018). In the same vein, Libicki (2017b) observed that the nonprofit organization must have a hands-on monitoring and response system to allow for real-time dealing with events and suspected breaches. The 360-degree security strategy's main valuable assets include the people and data/intellectual property (IP; Libicki, 2017b). The nonprofit organization needs to protect these vital assets by putting controls, processes, and technology to guard them. These controls, procedures, and technology, according to Cobb et al. (2018), are subject to constant assessments to guarantee a fully effective control mechanism.

During the 360-degree security strategy implementation, intelligence-led testing is crucial (Kholidy et al., 2016). The nonprofits must simulate every form of attack likely to be encountered and verify if their assets are adequately protected. According to Young and Drees (2018), next-generation testing should be directed by the existent attacks and threat vectors that malicious users and other external hackers employ. After the intelligence-led testing, nonprofit organizations must ensure that they improve security governance (Catota et al., 2018). Catota et al. asserted that nonprofit organizations must continuously review, improve, and evaluate their environments using managing risks, doing audits, and ensuring that the controls and testing mechanisms put in place are guarding the high-value assets. These studies' results are essential to my study because adopting a comprehensive, all-around in-depth approach to combating cyberattacks enables nonprofits to enhance their ability to respond to any form of malicious attack. The 360-degree security strategy creates an organizational culture where the nonprofits proactively defend their data resources and operations against attack rather than remaining reactive to the threat.

Additionally, Bordoff et al. (2017) emphasized the need for the nonprofits to train their staff about the best practices on security and substantiate third parties. The next course of action for the 360-degree security strategy is monitoring the incident response (Kholidy et al., 2016). As Kholidy et al. point out, this is an essential intervention because data breach reports indicate that many breach incidents remain unnoticed, sometimes for even more than six months. This prolonged period of up to six months and beyond unnoticed data breaches imply that hackers could be having all the freedom to access the data they want from their victims (Kholidy et al., 2016). Responding to Kholidy et al.’s observations, Garlinec et al. (2017) observed that proactive monitoring is critical if the nonprofit organizations have to feed into well-developed plans aimed at incident response. The devising of these plans must consider that training, simulation, and feedback all lead to an effective response whenever needed (Garlinec et al., 2017). During a penetration test, the tester may end up compromising a server, subsequently accessing data that is sensitive or elevate privileges for purposes of gaining system-wide access to the workforce knowing it (Bertoglio & Zorzo, 2017). For this reason, staff need awareness on how to handle such an event.

Nonprofits could also resort to cloud computing as a strategy to enhance cybersecurity (Hubbard et al., 2019). In this respect, cloud computing implies the technologies that rely on the Internet as a podium to guarantee users virtually ubiquitous access to extremely scalable, supple, and robust computing resources using online services hosted in data centers located off-site (Bidgoli, 2018). According to Nieuwenhuis et al. (2018), presently, enterprises of various sizes are shifting their IT systems “to the cloud” as a means of achieving effective and efficient operations. Apart from efficiency in operations, Wright et al. (2017) noted that nonprofit organizations can consider cloud computing as a strategy to enhance cybersecurity and achieve privacy goals. As already pointed out, most nonprofits tend to operate on a shoestring budget that eventually forces limited resources towards cybersecurity management (Jalali & Kaiser, 2018). However, according to Wright et al., cloud computing can play a significant role in supporting nonprofits to pay for the computing resources they require on a need basis, thus saving on money. Rathi and Given (2017) agreed with Wright et al. observation, noting that cloud computing hosts applications and services situated in off-site data centers maintained by an expert cloud service provider. Data centers' off-site location lowers the heavy burden that would otherwise face the nonprofits as they seek to install, regularly update, and maintain hardware and software (Rathi & Given, 2017).

Cloud computing's most crucial role is to present an immediate alternative for guaranteeing data security for nonprofits without requiring substantial upfront investment (Attaran, 2017). Data security is significant for cybersecurity as well as data protection fulfillment. The critical requirement for comprehensive data security laws, such as the General Data Protection Regulation and Data Protection Directive, require that organizations dealing with personal data should train their staff on the necessary technical and organizational measures on security (Dove, 2018). Such measures guarantee the protection of all personal data they store or process (Malgieri & Comandé, 2017). Fulfilling these requirements may not be possible unless a nonprofit implements adequate systems and safeguards that prevent their data from malicious disclosure or access. However, nonprofits find it difficult to comply with these general requirements because of their limited resources and technical skills to apply comprehensive on-premises security systems (Wright et al., 2017). In these instances, Rathi and Given noted that cloud solutions serve to offer a significant boost towards nonprofit data security without necessarily demanding higher technical skills, time investment, and cost.

Cloud systems guarantee greater security, especially for the poorly funded nonprofits, because some of the necessary security undertakings of cloud systems include end-to-end encryption (Baseri et al., 2018). The encryption covers both internally stored data and data on transit between the client organization and the cloud datacenter.

Additionally, Kajiyama et al. (2017) noted that cloud systems provide state-of-the-art physical security that includes 24-hour scrutiny, physical access controls, together with multiple-layered perimeter protection. Rossouw and Willett (2017) noted that cloud systems are required to comply with data protection standards, such as ISO 27002, ISO 27017, and ISO 27018, in addition to conforming to international security. These features ensure a great deal of robust cybersecurity infrastructure, much of which many nonprofits can afford to establish as part of their on-premises infrastructure (Rossouw & Willett, 2017).

Data Governance

Data governance refers to a companywide framework aimed at assigning rights that are decision-related and duties for purposes of adequately handling data as an asset of the company (Alhassan et al., 2016). Essentially, data governance's primary purpose is to make data a critical asset consideration of the firm (Alhassan et al., 2016). For nonprofits like churches and hospitals, their data volumes have been exploding following years of continued operations in their areas of jurisdictions (Lee, 2016). Data governance is vital to cybersecurity because it augments numerous protection lines for data at risk (Yang et al., 2019). According to Yang et al., data at risk involved data that would compromise the organization if it were to be accessed by unauthorized people. Identifying this type of data is crucial, bearing in mind that it is impossible securing all data for most organizations (Sarabi et al., 2016). The continued emergence of technologies aimed at helping nonprofits manage their increased load effectively may not be adequate. Nonprofits may not be aware of the existing data, where it sits, or how the organization's various units and other third-party entities use it (Pearce, 2017). Therefore, based on these aspects, Pearce justified the importance of data governance because of its gearing towards maximizing operational effectiveness by guaranteeing data value, enhancing decision-making, and enforcing regulatory compliance. Agreeing with Pearce, Rainie et al. (2017) asserted that data governance also helps nonprofits in their quest to minimize low data management risks. Many nonprofits, especially those well-established, such as the Red Cross, already have a superior data governance foundation. However, they seldom revisit their strategy even as they integrate newer data and analytics platforms (Rainie et al., 2017). Several data governance activities or pillars that nonprofits can consider for their safety exist.

The first data governance practice focuses on processes, policies, standards, and procedures (Rainie et al., 2017). According to Rainie et al., the nonprofit organization's data governance, just like in other organizations, must reflect the firm’s strategic direction and the desired outcomes regarding data management, information security, architecture, and data modeling. Yeong and Suh (2018) opined that organizations such as nonprofits must consider the evolving processes, standards, policies, and procedures in their efforts to pursuing effective data governance. In particular, Yeong and Suh argued that nonprofits implementing new data platforms must, first of all, consider process automation. Newer platforms with a processing power for large data volumes can make possible more interactive, experimental, and evolutionary analytics (Yeong & Suh, 2018). When the nonprofits eventually achieve their enhanced scale and process complex information directly, they ultimately improve their potential to undertake data management operations (Kuerbis & Badiei, 2017). According to Kuerbis and Badiei, many processes, such as data quality validations or metadata discovery, may become enhanced due to being automated by way of cognitive technologies.

Data governance practices must be equally democratized if, at all, the nonprofits intend to achieve positive outcomes (Parks et al., 2017). In the nonprofits, the scale and the complexity of the data always increase, and consequently, this forces responsibility for managing the data to shift owners (Park et al., 2016). As such, Park et al. held that it is essential that the nonprofits' management equip the organization with the necessary collaborative tools, standards, processes, and procedures to guarantee effective management. Finally, under the focus on operations, policies, procedures, and standards, it is always essential for the nonprofits' management to appreciate that standards and procedures continuously evolve to pave the way for new architectural prototypes (Williams & Woodward, 2015). Echoing Williams and Woodward, Prakash and Singaravel (2015) added that nonprofits continuously operated in an environment where their analytical and operational landscapes kept changing. The nonprofits have to store copies of the data they handle in separate physical locations, making management more difficult and predisposed to security compromises. For this reason, thus, nonprofits are expected to advance their procedures and standards for purposes of data security and architecture (Prakash & Singaravel, 2015).

The second data governance practice focuses on organizations, roles, and responsibilities (Garlinec et al., 2017). These authors argue many nonprofits have come up with data governance arrangements that encompass well-defined duties and roles to facilitate and oversee data management processes. However, Burns et al. (2017) had a different view from Garlinec et al., noting that newer platforms are emerging and higher chances of organizations, responsibilities, and roles also changing. Thus, the nonprofits must put several considerations into place. They must consider extending data governance towards development (Burns et al., 2017). More governance will be necessitated by accountability for data beyond the primary sphere of data management to the software life cycle development (Kuerbis & Badiei, 2017). As such, Anand et al. (2018) expounded on Kuerbis and Badiei's assertions, noting that this would lead to a more proactive process of data governance.

On the other hand, data governance would lower the necessity of fixing production platform issues. Apart from extending data governance towards development, there is also a need for nonprofits to have upskilling stewards in their data governance endeavors (Anand et al., 2018). Such stewards will bring in technical credence to accommodate emerging technology alterations such as big data, cloud-enabled platforms, microservices, and streaming data (Anand et al., 2018). According to Anand et al., nonprofits can offer training that would help the stewards effectively perform their duties on modern data platforms. Finally, consideration requires direction on data security functions (DiMase et al., 2015). Echoing DiMase et al., Stewart and Jürjens (2017) observed that using multiple channels to access information both within and outside the firm increases the data security risk levels. Mainly, the nonprofits must introduce disruptive technologies as well in their bid to put a check on data usage and access (Stewart & Jürjens, 2017). Reviewing these numerous studies, I established rich information that helped develop practical IT security strategies that nonprofits used to protect information from cyberattacks.

Security and Privacy

In a nonprofit organization, privacy is described as the capability to guard sensitive information (Martin & Murphy, 2017). For nonprofits such as hospitals, privacy entails safeguarding personally identifiable health care information at their disposal (Abouelmehdi et al., 2017). According to Adams (2017), nonprofits safeguarded personal information only after the entrenchment of storage and transportation processes within security measures. Adams particularly suggested a raft of measures that nonprofit organizations can consider in their quest to uphold security and privacies to guard against data breaches.

First, nonprofits should consider systematic and effective ways to discard personal information that they have been holding, particularly when that information is not required anymore in its simple forms (Adams, 2017). Explanations by Maras (2015) appear to be in tandem with those of Adams, noting that the absolute amount of data exchanged in a nonprofit organization grows exponentially. The exponential growth creates risk on the security of the data because, according to Maras, even highly dynamic systems may fail to secure the privacy of such information, especially with the risk of data streaming from new objects and devices. Samani et al. (2015) suggested that organizations such as nonprofits can lower the risk of their new servers being targeted by hackers by simply maintaining diligence in adhering to procedures discarding data. In the current internet of things (IoT) environment, nonprofits can be at a higher danger of leaving their privacy exposed if their data handling and management practice remains inconsistent (Samani et al., 2015).

Second, nonprofits must also be aware that the public-private areas of policies and protections sometimes become blurred as far as data exchange context is concerned (van de Pas & van Bussel, 2015). This blurring means that public institutions' policies to limit data collection may not exist in nonprofit organizations. For example, individuals within society may not choose to disclose their personal information to nonprofits; however, such disclosure increases the risk of exposing individuals' private information to hackers and data breaches.

Third, nonprofits need to explore the de-identification approach as a way of guarding their security and privacy against data breaches (Quirós et al., 2015). Deidentification refers to a traditional technique of prohibiting confidential information disclosure by declining any detail that can recognize an individual (Abouelmehdi et al., 2017). The de-identification technique, according to Abouelmehdi et al., works by removing particular identifiers of the data. However, even with these measures, Kayaalp (2018) argued that attackers can still access additional external information assistance for the de-identification. In particular, attackers target such nonprofits as hospitals where big data is involved. Emphasizing his point, therefore, Kayaalp insisted that de-identification is not a sufficient approach through which nonprofits can protect critical data privacy. Instead, Kayaalp suggested the need for organizations like nonprofits to come up with efficient privacy-preserving algorithms as a means of mitigating the re-identification risk. Rajendran et al. (2017) mentioned k-anonymity, l-diversity, and t-closeness concepts that organizations like nonprofits may need to consider in enhancing this traditional technique. The k-anonymity technique works so that as the value of k increases, the re-identification probability will go lower (Rajendran et al., 2017). Nonetheless, Quirós et al. (2015) pointed out that this technique may produce data distortions in the organization, leading to more significant information loss. Moreover, Quirós et al. explained that excessive anonymization risks making the data disclosed less useful, especially to the recipients, as some analysis may end up providing erroneous and biased results.

Fourth, nonprofit organizations need to re-evaluate their privacy processes and policies by engaging all their stakeholders (Pouloudi et al., 2016). For nonprofits like hospitals, stakeholders' engagement should include nurses, physicians, insurance companies, administrators, and all other business associates (Pouloudi et al., 2016). Explaining the logic behind this reasoning, Parks et al. (2017) mentioned that when stakeholders drawn from varied areas are engaged in the organization’s privacy practice, the likelihood of negative consequences is limited. According to Parks et al., mere privacy policies only can prove to be virtually meaningless and highly superficial to a nonprofit organization unless the stakeholders get involved in the development, monitoring, and enforcement of the same. Agreeing with Parks et al., Lim et al. (2018) added that nonprofits need real privacy protection and advocacy put up as part of the process making up the organization.

Moreover, Lim et al. (2018) advised that organizations such as nonprofits must allow the senior management to be at the forefront as far as real privacy protection and advocacy is concerned. Executives leading a nonprofit such as a hospital must understand the importance of minimizing the unintended consequences if they seek to reduce the imbalance challenge (Abouelmehdi et al., 2018). In general, these measures help determine critical detail that would effectively establish practical IT security strategies against cyberattacks on nonprofits, thus, supporting my research question.

Job Roles Associated with Information System Security Managers

The role of information security managers is at the center of much attention in recent years. ISSMs play influential positions in the fight against cyber threats, the enforcement of security policies, and employee management**.** According to Al-Taie et al. (2018), the CIO undertakes six significant roles: strategizing for IT-based innovation and business process redesign, serving as relationship architect with noteworthy IT service providers, and integrating processing, information, together with decision support. The CIO's other roles include educating top management about IT and its value to the organization, utility provision of IT infrastructure services, and serving as the organization’s information steward for operationally reliable systems and high-quality data (Al-Taie et al., 2018). Tumbas et al. (2018) summarize the CIO's role as the institutionalized domain in charge of holding jurisdiction regarding innovation with digital technologies. Typically, Tumbas et al. characterized the CIO's behavior as structured following IT professional norms, including integrating systems and maximizing constant business tasks.

The CISO undertakes the role of aiding customer relationship maintenance and increasing retention through protecting company reputation and confidential customer information (Lanz, 2017). Additionally, Lanz stated that the CISO develops and monitors compliance with cybersecurity procedures and policies and monitors and evaluates its technical activities to manage technology-related risks accordingly. Other CISO roles include complying with technology-related regulations, preparing tests and reports regarding business resiliency, and managing third-party service providers' organization-wide supervision. CISOs also lead management investigations on the general use of technology in the organization and serve as the primary contact about law enforcement (Lanz, 2017).

Transition and Summary

In section 1 I covered the introduction, describing the study's background information. I included 12 main elements in the section that broadly covered the foundation and the scope of the study. The areas in this section included the problem's background, the problem statement, purpose statement, the nature of the study, the research questions, the conceptual framework, the operational terms, assumptions, research limitations, delimitations, the significance of the study, and finally a summary of professional as well as scholarly works of literature reviewed.

In section 2 of the research study, I covered participants in the study and the research method, design, population sampling, research ethics, data collection instruments, data collection techniques, data analysis, and reliability and validity. I also covered elaborate details about the methodology and the research process to be adopted. In section 3, I presented the findings, applied the findings to professional practice, covered the social change implications, provided recommendations for action, provided recommendations for further study, offered reflections, and finally summarized and included the study's conclusion.

Section 2: The Project

In this study I sought to explore cyberattack strategies for nonprofit organizations. Section 2 of this project illustrates elaborate details about the methodology and the research process that I adopted. Overall, this section includes the purpose statement, the researcher's role, details about participants, the research method and design, and the research population. Other topics include sampling method, data collection, organization and analysis, and a reflection on reliability and validity.

Purpose Statement

The purpose of this qualitative multiple case study was to explore the strategies that ISSMs at nonprofit organizations employed in protecting against cyberattacks. The specific population encompassed IT managers and directors of IT in charge of security management in nonprofit organizations in Maryland, the District of Columbia, and Virginia. I conducted the study at different sites using participants' information. This study's social change implications are that people in charge of or engaged with nonprofit organizations could decrease identity theft and improve safe environments. The impact of social change could be far-reaching because victims of cyberattacks suffer financial losses, operational disruptions, reputational damage, and legal ramifications, among other ill effects. With the pervasive nature of cyberattacks, many individuals have suffered from stolen and misused data.

Role of the Researcher

Qualitative research practice requires the researcher to assume the instrument's role engaged in primary data collection (Daniel, 2018). I was the primary data collection instrument in my study. Essentially, qualitative researchers need to develop themselves (a) to become research instruments for collecting data from the research sample population; (b) design, interpret, and undertake qualitative data analysis; and (c) present findings of the study while taking into consideration ethical and high-quality standards (Marshall & Rossman, 2016).

A researcher's personal experience influences the studies they conduct (Thistoll et al., 2016). I considered myself experienced as the researcher in this study in that I have studied IT to higher education levels. I have a good understanding of data security and management and familiarity with some of the strategies used for data security organizations. I focused on mitigating the effects of my experiences as the researcher towards my study to avoid bias. I lived in Frederick, Maryland, and I worked in IT. I had no professional relationship with the participants in the study. These factors could have alleviated the participants' concerns regarding revealing sensitive details or allayed reluctance to participate in the study.

Bias had the potential to influence my study. Practices aimed at mitigating bias in qualitative research include using multiple interviewees, data triangulation, implementing member checking, and following an interview protocol (Ranney et al., 2015). I used data obtained from interviewees as well as from organizational documents to carry out methodological triangulation.

I conducted the interviews to offer the participants an opportunity to explain cybersecurity issues and incidents in their organization freely. Adopting the interview protocol helped me get a critical understanding of the research topic. According to Henry and Foss (2015), interview protocols are essential when employing the interview method because they offer the researcher guidance to collect reliable data.

As the researcher in this study, I followed the interview protocol (Appendix) to guarantee that I maintained uniformity during the interview process. Researchers must strictly adhere to the interview protocol to ensure that they avoid biasness in their findings (Ngongo et al., 2015). As the researcher, I was required to adhere to ethical principles and guidelines as stipulated in the *Belmont Report* (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1979). These principles and guidance are designed to protect human subjects who are taking part in research, to cause no harm and treat participants fairly (Adashi et al., 2018). I completed the National Institutes of Health's (NIH) training on Protecting Human Research Participants to better understand ethical challenges and participant protection. Participation was voluntary and without coercion. An interview protocol is crucial in aiding the interviewer in preparing for the interview, including ensuring that the questions are known and determining information that is most critical to the research (Majid et al., 2017).

Participants

I chose the participants in this study from among IT managers and directors of IT drawn from five nonprofit organizations. I selected participants who had experience in data security and risk management. In this study, participants were required to have experience in data security and risk management and at least 5 years of working in nonprofits' IT department. Participants' eligibility in a study goes with their experience and their knowledge concerning the topic under investigation (Akaeze, 2016). Researchers must have clear principles and criteria to guide selecting participants in a research study (Daniel, 2018). The importance of such clear principles accords researchers the opportunity to appraise the research findings and the extent of transferability. Gaus (2017) observed that a researcher’s use of participant selection criteria helps ascertain the participants' credibility, accurate identification, and description.

Morris and Rosenbloom (2017) explained that researchers require Institutional Review Board (IRB) permission before contacting participants in their study. I searched the Tax-Exempt World website, a searchable repository that is freely accessible to the public and lists all the nonprofit organizations in America. I selected five nonprofit organizations from the website that met my research criteria and reached out to the organizations’ contacts. I sent an email to the contact persons identified on the website. In the correspondence, I communicated my intentions to research the organization including the aim and objectives. I requested the potential participants to contact me using my attached email address. According to Hampton et al. (2019), although a research study can have between four and fifteen participants as a desirable number, the focus of any research should always be to gather dense and rich data. The total number of participants should not be a question of concern but rather the richness of the eventual data. A sample range of three to eight applies suitably in case studies (Yin, 2017). After getting approval from Walden University and the participants’ acknowledgment correspondence expressing willingness to participate, I embarked on building a working relationship with the participants with the organizations' gatekeepers' help. In line with Pelosi's (2015) observation, I communicated with the potential participants to establish mutual trust to build confidence. According to Pelosi (2015), creating open communication with the research participants is critical as it gives the parties assurance of confidentiality. To create open communication, I (a) established a mutual feeling of friendliness and highlighted the common interests that we shared; (b) described the topic of research, my interest regarding the study, answered questions from the participants, and ensured the participants felt free and easy; (c) reassured participants that data integrity would be upheld throughout the research process, and (d) reemphasized the participant's confidentiality. I also (e) ensured positive and professional interaction by being polite and maintaining a nonjudgmental attitude; and (f) actively listened and engaged with the interviewees for the entire sessions. When research participants develop confidence in the researcher, they trust the working environment, which enhances credibility in general (Pelosi, 2015).

Research Method and Design

Method

I chose the qualitative method for use in this study. The qualitative research method was ideal for this study because this methodology suits research aimed at exploring and understanding the meaning individuals or groups accord human or social problems. Qualitative research is exploratory and is used to understand human behavior, groups, phenomena, and individuals (Cavalcanti, 2017). Exploratory researchers use interpretive approaches in the collection, analysis, and interpretation of the research data.

The objective of exploratory research is determining answers to the *how* and *why* questions of a phenomenon. The exploratory analysis does not concern itself with the *what, where,* and *when* of a phenomenon (Gaus, 2017). Qualitative studies often result in tangible outcomes by using well-documented data assembling and analysis practice (Shukla, 2016).

Unlike the qualitative research method, the quantitative research method relies on statistical data to draw findings after the analysis (Hammarberg et al., 2016). According to Cerniglia et al. (2016), quantitative research premises include probability and statistics. In my study, the objective involved no hypotheses testing or seeking of any statistical data. Mostly, I did not select a quantitative research method because I was planning on neither hypothesis testing nor statistical data analysis.

The mixed methods approach focuses on combining, congregating, enhancing, and demonstrating the research outcome using quantitative and qualitative methods (Wardale et al., 2015). The combined approach makes mixed methods research more useful when it comes to designing, building, and testing theories, in addition to completing the inductive and deductive analysis in studies centered on a central research question and hypotheses (Wardale et al., 2015). Cameron et al. (2015) established that mixed-methods research accords the researchers with the opportunity to join the experiences of participants and empirical data to allow for the determination of existing relationships between particular variables. Because I was specifically seeking the insights of participants in my study, the choice of mixed methods research, which focuses more on examining combined experiences, relationships, and hypotheses between variables, was not ideal. I did not choose the mixed methods study for this research.

Research Design

For this research I adopted the qualitative multiple case study design as the appropriate choice to explore strategies that nonprofit organizations used to protect against cyberattacks. Qualitative research designs exist in different types, including ethnography, case study, and phenomenology (Mohajan, 2018). These approaches involve similar research features regarding the research problem, data, data analysis, questions, and reporting results. The ethnography design type of qualitative investigation applies mainly to the study of people and cultures. Applying ethnography in research requires observing the study participants while in their natural habitats to deeply understand their experiences, perceptions, creation, and navigation of the social world (Wels, 2015). The researcher collects the data in rich context from numerous sources of evidence within a real-life situation (Dasgupta, 2015). I did not choose the ethnography research design because the study did not involve group culture observations. The phenomenology design examines the meaning of lived occurrences that a person or individuals, as a group, have collectively experienced (Mohajan, 2018) and also helps the researcher separate biases and assumptions (Larkin et al., 2019). I did not consider the phenomenology design for this research because the purpose did not target lived experiences of the participants.

The case study design focuses mainly on exploring bounded systems over time (Corti & Fielding, 2016). The exploration of bounded systems happens in an elaborate, in depth data collection exercise. Case studies serve best for their flexibility when used alongside the qualitative research methods (Morgan et al., 2017). According to Corti and Fielding (2016), the case study design makes it possible for a researcher to obtain a more exhaustive understanding regarding a given issue within a specific time. Because I intended to use greater flexibility in my quest to learn about some of the strategies that ISSMs at nonprofit organizations employ in protecting against cyberattacks at nonprofits, I chose to adopt the case study design. The qualitative case study design integrated my pragmatic worldview, GST conceptual framework, a small sample size, data collection methods, analysis, and the time constraints limiting the conduction of a doctoral study in a given timeframe.

According to Saunders et al. (2018), a researcher meets data saturation when the resultant interviews involving research participants yield no new themes. Qualitative researchers can avoid such a situation by interviewing more participants until they achieve data saturation (Elman et al., 2016). Boddy (2016) noted that qualitative researchers may stop interviewing additional study participants when further interviews provide no new details regarding the research topic. In this research, I recruited participants and collected data from them until I could not establish the emergence of any new themes about the strategies that ISSMs at nonprofit organizations employ in protecting against cyberattacks at nonprofits.

Population and Sampling

Research experts advise the ideal number of participants that should be involved in a sample. Boddy (2016) observed that qualitative research lacks specific rules on sample size. Boddy also quoted another study by Sandelowsky (1995), whose findings observed that sample sizes of 50 are substantial for qualitative research work. Other researchers' recommendations allow for different sampling sizes as per the research criteria (Williams & Needham, 2016). In this study, I chose the participants from among ISSMs drawn from five nonprofit organizations freely accessible to the public in Maryland, the District of Columbia, and Virginia. Each nonprofit is a single case in a multiple case study. I believed that the interviews and the organizations published and non-published documents would yield enough data for triangulation.

There are two sampling techniques: probability and nonprobability (Lucas, 2016). A purposive sampling technique is a non-probability sampling methodology that gives the researcher the freedom to choose qualified participants to inform the research question (Benoot et al., 2016). According to Hennink et al. (2017), a purposive sampling technique facilitates the researcher to pick participants intentionally using unique individual characteristics concerning the subject under study. Ridder (2017) argued that the use of purposive sampling fits appropriately with case study research because it allows determining the participants who will be useful in answering the research question.

Eriksson (2017) identified purposive sampling as significant especially when dealing with homogeneous groups of participants because it enhances the exploitation activity of any research study. I chose homogeneous purposive sampling for this research because it enhanced the exploitation activity during the research study. The research participants had shared characteristics of being ISSMs with experience in data security and risk management, and with experience not below five years working in the IT department of nonprofits.

Data saturation use in research constitutes a guiding principle in testing sufficiency regarding purposive sampling (Hennink et al., 2017). According to Constantinou et al. (2017), data saturation arises once the data become redundant or begins to replicate. Researchers embark on a precise data saturation process to ensure no overlooking of different meanings, new data, new issues, or new coding that crops up. I made data saturation my main focus. I did not stop data collection until I noticed participants beginning to duplicate information or the information offered lacking value to the research topic.

Data collection was conducted virtually to avoid social interaction and prevent Coronavirus's spread as an alternative to a private office. I used the nonprofits' IT security strategies against Cyberattacks Questions (see Appendix) to investigate the participant's views and ideas regarding cybersecurity practices in their organizations. When the interview setting is relaxed, participants will be encouraged to ask questions and respond freely (Qu & Dumay, 2011).

Ethical Research

After getting approval to proceed with the Walden IRB research (approval no. 09-18-20-0682479), I selected the targeted nonprofit organizations to be involved in the study. I sent via email an informed consent form, asking those meeting eligibility criteria to complete the form to ascertain their willingness to engage in the study. The critical information included defined the study's purpose, the researcher's role, participation criteria, and withdrawal process in the consent form. Other details in the consent form included the study findings' publication intention and the data safeguard mechanism. I emphasized to the participants about there being no forced participation but rather only by voluntary means. I reminded the participants of the right to stop and withdraw their participation at any time. No explanation was required to withdraw other than a mere email notifying the researcher of the decision to quit.

Informed consent is a crucial aspect of any given research study. A researcher will have to balance participant interaction to uphold all ethical requirements expected of a research study (Humphreys, 2015). The researcher must ensure the informed consent process does not violate the participants' rights or respect. Consent ensures full adherence to all necessary ethical standards (Greenwood, 2016). As the researcher, I followed Walden University IRB's ethical and legal requirements to avoid harming the research participants. Safety, dignity, and study participants' voice are essential in guaranteeing ethical practices when undertaking qualitative research (Wallace & Sheldon, 2015). The informed consent states that all participants in the research do so voluntarily. As clearly stated in the informed consent form, participants did not receive any incentives in the form of payments for them to enlist their participation in the study.

The confidentiality of research participants must always be maintained to guarantee the study's integrity (Wallace & Sheldon, 2015). Yang et al. (2018) noted that the use of unique identifiers to represent the study participants guards the participants' professional status. I used letters and numbers for purposes of identifying participants on both the transcripts and the research log. I assigned codes to the participants based on their order of interview so that code ‘M 1’ represented the first interviewee, code ‘M2’, the second one, and so forth. I was the only person with access to data from the study. I stored the data in a password-protected external drive, which was kept safe for five years to guard against the participant’s confidentiality.

Data Collection

Instruments

As the researcher, I assumed the primary data collection instrument's role and collected data in the natural setting. According to Stacey (2016), researchers undertaking qualitative studies assume primary data collection instruments' role. Collecting qualitative data requires establishing trust with participants, which means that the researcher is the data collection instrument expected to develop a strategy that will develop credibility with participants (Daniel, 2018). Collecting data in the natural setting helps researchers conduct inductive and deductive data analysis with regards to themes and patterns establishment (Fletcher, 2017).

Data collection in qualitative research may be in the form of semistructured interviews and document analysis (Akaeze, 2016; Conrad & Tucker, 2019). According to Van der Berg and Struwig (2017), semistructured interviews are valid for data collection. As Farooq and de Villiers (2017) noted, open-ended questions offer the opportunity for a researcher undertaking a case study to have great insight into the specific aspects involved. The interview questions that I used were open-ended to give room for more significant interaction that included the participants. I analyzed documents from the organizations to perform methodological triangulation. Besides the interviews and observation, I used the nonprofit's published and non-published documents such as the organization bylaws, strategy plan, brochure, policy, training logs, and System security plan. I used interviews as an instrument for collecting data. I used a pre-determined set of interview questions as the data collection instrument (Appendix). Every interviewee responded to the same set of questions and in the same order to ensure consistency in the eventual data collected.

A researcher can get different answers and interactions during an interview session if they ask different participants the same interview questions (Cataldi, 2018). Pandey and Chawla (2016) observed that semistructured interview formats allow participants to have an in-depth understanding of the research topic. They also noted that the adoption of semistructured interviews provides an accessible, flexible, and intelligible approach to data collection. Muhammad (2018) illustrated the degree of effectiveness of qualitative studies using semistructured interviews. Essentially, using semistructured interviews, a researcher can divulge hidden aspects that are characteristic of human and organizational behavior because participants' responses are in such a manner that they are best suited for the interview question.

I posed the same interview questions to all the participants to ensure credibility and reliability using an interview protocol (Appendix). According to Azungah (2018), posing the same interview questions to all research participants helps discover themes. When asking the same questions sequentially, the researcher can undertake efficient data analysis and draw comparisons of the responses (Akaeze, 2016). Researchers need to avoid leading questions because, according to Teixeira et al. (2017), such questions promote bias.

Methodological triangulation offers a researcher an opportunity to mitigate bias as the researcher gains the capability to view the data from various perspectives. They may consider a phenomenon in multiple ways (Fusch et al., 2018). Utilizing methodological triangulation will further enhance flexibility in establishing trends throughout the data analysis process (Mason, 2018). Using multiple data sources as a target of methodological triangulation enhances the study's credibility, validity, and reliability (Fusch et al., 2018). I combined participant interviews with analyzed organization documents such as the nonprofits' published and non-published documents: bylaws, strategy plan, brochure, training logs, and System security plan, training logs, software acquisition documents, and policy documents. Conferring to Das et al. (2018), archived data such as recordings and documents lead to valuable qualitative research data. A researcher's analysis of archival documents combined with observations and interviews allows for the revelation of research themes (Davidson et al., 2019). The methodological triangulation, which involves using multiple data forms, enables a researcher to understand the fact they are studying. According to Fusch et al. (2018), utilizing a combination of two data collection methodologies makes the data more reliable, which in turn makes the case more understandable. Methodological triangulation further facilitates the probing of patterns within the data, enabling the researcher to interpret multiple perspectives. Adopting methodological triangulation boosts confidence towards the study’s findings because it entails using various sources that, in turn, help the researcher mitigate research biases (Azungah, 2018).

I applied member checking in the interview process to enhance research validity and reduce bias. Through member checking, Daniel (2018) argued that the researcher stands a chance of achieving rigor or thoroughness in case studies. The participants had the opportunity to review and confirm my interpretation of the initial meeting before I proceeded. As Daniel noted, member checking presents an opportunity through which the researcher can verify the level of accuracy in a participant’s response. Member checking further serves as a quality control process, where the researcher can confirm, clarify, and supplement data obtained from a qualitative research interview (Iivari, 2018). I used a pre-determined set of interview questions as the data collection instrument. Every interviewee responded to the same set of questions and in the same order to ensure consistency in the eventual data collected (Appendix).

Data Collection Technique

This study used interviews as the technique for collecting data. Interviewing entails a data collection method where individuals' experiences are mined through a question-answer session to establish a composite understanding that broadens our professional knowledge (Quinney et al., 2016). Researchers utilize interviews to capture participants’ experiences in qualitative studies (Holland, 2017). Researchers choosing the option of a conversation as the technique to engage with participants might use structured, semistructured, or unstructured versions for data collection (McTate & Leffler, 2017). I used semi-structured interviews and document analysis in this study. I looked for organization documents to analyze from the organizations' respective websites and requested private data from nonprofit organizations. Among the documents that I searched for in the websites and use for data collection included training logs, software acquisition documents, and system security plans and policy documents.

Researchers using semi-structured interviews adopt a guide for the interview where listed questions focus on capturing the interview’s social cue (Van Rooy et al., 2015). Akaeze (2016) explained that researchers adopting semi-structured interviews depend on the general research question to guide the data gathering process. The advantage of semi-structured interviews includes the flexibility of using follow up and supporting questions, which ensures the drawing of rich data about a phenomenon. Additionally, semi-structured interviews involve open-ended questions that grant participants the opportunity to freely respond using their own words and based on their worldview (Kallio et al., 2016). Semi-structured interviews also benefit researchers through, according to Kallio et al., an opportunity to develop relationships with participants. Such a relationship further makes it easy for the researcher to address participants’ arising concerns or questions (Newton, 2017).

Structured interviews entail a more rigid configuration regarding the wording and sequencing of questions (Doll, 2017). I did not choose a structured interview in this study because it entailed rigorous procedures that are more standardized and with ordered questions. On the other hand, unstructured interviews require researchers to ask different questions to different participants based on the researcher’s judgment (Mcintosh & Morse, 2015). I did not choose unstructured interviews because, practically, the interviewer has the discretion to direct the interview process in any direction they prefer, which, in essence, facilitates bias (Mcintosh & Morse, 2015).

According to Holland (2017), however, semi-structured interviews have the disadvantage of being lengthy and costly. The unstructured methodology, coupled with the complexity of data, and the excessive details attributed to participants, makes it quite challenging to use the method. Moreover, using semi-structured interviews increases the chances of researcher bias, which may, in turn, influence data interpretation unfairly (Brown & Danaher, 2017). I invited participants via email, asking them to take part in the study. The participants received, reviewed, and eventually approved a consent form before participating. The consent form explained the withdrawal process, disclosure of incentives, and the mechanism for safeguarding data.

I used the member checking process to make sure that I achieve response validity. I summarized all the interview responses for member checking. According to Madill and Sullivan (2018), member checking facilitates researchers in their quest to investigate and fit their interpretation relatively with the participants' responses. I engaged in member checking conversation with the participants to allow the participants to review and confirm my interpretation of their responses. Participants were asked to edit, simplify, explain further, and comment on the summary of their response to make sure my understanding of their viewpoint.

Data Organization Techniques

Researchers often use software to track data and organize it accordingly (Che-Hung et al., 2017). After the interviews, I transferred the raw data into NVivo. I also removed any possible personal or identifiable details that could quickly reveal the participants' actual identity. I had a folder with labels relating to each case study, where I stored the transcripts, notes, and interview recordings in an external drive only accessible to me for five years. I did as a measure to enhance the participants' privacy and security.

My intention in undertaking data analysis was to achieve a more in-depth evaluation of the themes and patterns in the interviews. I uploaded, organized, and analyzed the transcribed interview data with the help of NVivo software. As computer-assisted software for qualitative data analysis, NVivo software aids data collection and the subsequent management and analysis. Using NVivo software, I recognized meaningful units, expanded emergent themes, managed data, and undertook triangulation.

I loaded the nonprofit organizations' published and non-published documents such as the organization strategy plan, brochure, and policy into NVivo software for purposes of conducting methodological triangulation. The methodological triangulation presented me with a chance to use multiple sources of qualitative research data. My use of methodological triangulation helped me attain flexibility in terms of determining trends in the course of data analysis. Multiple data sources provide methodological triangulation to support a plausible case for the soundness of research findings, concluding remarks, and recommendations (Heesen et al., 2016).

I used data coding to simplify the process involved in comparing and recognizing patterns. In coding the qualitative data, I investigated study data for categories, ideas, and common themes. The coding facilitated analysis, organization, and a comparison of data to enable the extraction of meaningful information. I applied a coding process that categorized data based on source types using archived documents and interviews to determine the emerging themes (Young et al., 2018).

When using NVivo to code data, nodes have to be created (Ballaro & Polk, 2017). A node constitutes the references collected about a specific theme, person, area of interest, or place. I used transcriptions, logs, and notes to discover inherent themes, patterns and deduce meanings based on the participants' responses. I took interview notes in the form of a research log to ensure my study's conformability, validity, and reliability. Mohajan (2018) opine that researchers rely on research logs purposely to capture data and scrutinize assumptions and actions that are thematic in a given study. Research logs further offer a valuable audit trail to ensure conformability and enable the researcher to recognize and reflect on the potential challenges likely to affect the research (Mohajan, 2018).

Data Analysis Technique

According to Assarroudi et al. (2018), data analysis constitutes a process of classifying the information gathered during interview sessions, or by observation, or the review of visual and written documents. I embarked on transforming raw data and organizing it accordingly to achieve rigor in data analysis. I ensured adherence to data analysis by meeting all standard principles, including interviews transcription, comprehensive analysis of the phenomenon under investigation, member checking data coding development, and determining links to themes. Nowell et al. (2017) explained that the data analysis process comes after the researcher accesses the field, gathers data, and transcribes it.

I uploaded, organized, and analyzed the transcribed interview data with the help of NVivo software. As computer-assisted software for qualitative data analysis, NVivo aids data collection and the subsequent management and analysis of such qualitative data as written and audio content (Woods et al., 2016). Using NVivo software, I recognized meaningful units, expanded emergent themes, managed data, and undertook triangulation. Using both interview and document analysis data, I achieved methodological triangulation and attained flexibility in determining data analysis trends. Multiple data sources provide methodological triangulation to support a plausible case for the soundness of research findings, concluding remarks, and recommendations (Nowell et al., 2017).

I used data coding to simplify the process involved in comparing and recognizing patterns. In coding the qualitative data, I investigated study data for categories, ideas, and common themes (Wu et al., 2016). The coding facilitated analysis, organization, and a comparison of data to enable the extraction of meaningful information. I applied a coding process that categorized data based on source types using archived documents and interviews to determine the emerging themes (Erlingsson & Brysiewicz, 2017).

Reliability and Validity

Introduction

Generally, qualitative research must establish the data's trustworthiness to achieve reliability and validity (Roberts et al., 2019). It is critical for a researcher to pay close attention when designing a study to ensure the findings are well applicable. Using transferability, dependability, and confirmability facilitates establishing trustworthiness and improving a study's quality (DeGama et al., 2019). Qualitative studies to attain the much-needed trustworthiness must be credible, dependable, confirmable, and transferable (DeGama et al., 2019).

Reliability

In qualitative research, reliability refers to how the data are producible and stable (Leung, 2015). Member checking is an essential element to determine if the researcher investigates and accurately interprets the participants' responses (Madill & Sullivan, 2018). I provided an opportunity for the participants to verify my interpretation of their interview responses to ensure accurate findings. Furthermore, member checking disseminates the analyses and participants' research responses to capture the meaning and increase data reliability (Fusch et al., 2018). According to Robins and Eisen (2017), triangulation equally results in reliability in research. Triangulation employs numerous data support for purposes of sustaining interview data and ensuring fidelity regarding the research outcomes. I used multiple data collection sources such as published and non-publish documents and semistructured interviews to ensure the findings' reliability.

Validity

Dependability

Dependability implies the degree to which the research findings are ethically and accurately produced (Van der Ber. & Struwig, 2017). Researchers achieve data dependability using member checking as it helps in ascertaining that their personal biases do not influence the data collected (Akaeze, 2016). In this study, I authenticated conclusions using member checking as well as triangulation methodologies. In terms of member checking, I mainly disseminated the interpretations and participants' research responses immediately after the data collection process, inviting them to validate them. Regarding triangulation, I crosschecked all data resulting from the interview and document analysis. I stuck to data attributed to the research participants and did not consider personal opinions that were likely to result in biases.

The significance of dependability lies in the fact that it enhances the trustworthiness of findings (Nowell et al., 2017). I achieved dependability in my study with audio-recording and writing down responses during the interview. I further transcribed the information and used Nvivo software to analyze the resultant data.

Credibility

Credibility implies the degree or extent of objectivity and impartiality regarding the research's findings (Bradshaw et al., 2017). Credibility ensures that the researchers effectively match the participants' opinions with the eventual outcomes (Colorafi & Evans, 2016). According to Turner and Baker (2019), researchers pursue credibility in their studies as a means of achieving the necessary trustworthiness and integrity. Credibility is an essential aspect of internal qualitative data and entails establishing plausible research findings as per the research participants' perspective (Noble & Smith, 2015). A study considered credible implies that reviewers not involved in the study acknowledge its findings and that the findings remain applicable to other settings or groups (Noble & Smith, 2015).

Iivari (2018) described member checking as a quality control procedure undertaken in qualitative research to enable the researcher to confirm, explain, or boost the accuracy of the accuracy relating to the interview data collected. Member checking ensures adequate verification of the data obtained through interviews. Daniel (2018) noted member checking provides room for participants to validate response portrayal.

Transferability

Transferability refers to the ability to have the research findings generalized to a broader population. Achieving transferability requires a qualitative researcher to find meaning for an individual involved in the research (Gammelgaard, 2017). The use of purposive sampling, as Venkatesh et al. (2016) point out, could enhance transferability. Additionally, methodological triangulation helps in improving transferability (Fusch et al., 2018). My research structure included focused sampling and a comprehensive outline of the research assumptions, delimitations, and limitations. The structure provided adequate context for establishing this study's transferability by other researchers. I recorded the research results so that other researchers can replicate them by using thick descriptions to illustrate participant data and including raw examples of data. I used methodological triangulation in addition to maintaining a case study database that included raw, themed, sorted, and interpretive data.

Confirmability

Research confirmability refers to how others can corroborate the research outcome (Muhammad, 2018). Researchers may use reflexive journals, transcript recording, and review, member checking, as well as note-taking in the interview process for capturing the audit trail for purposes of ensuring qualitative research confirmability and dependability (DeGama et al., 2019). Confirmability makes sure that the researcher signifies the participants' responses as opposed to the researcher's bias. I achieved confirmability and dependability by recording transcripts, reviewing them, and conducting member checking and taking notes throughout the interview process.

Transition and Summary

In section 2, I covered numerous essential elements that constitute this study, including restating the purpose statement and elaborating on the researcher's role. I also discussed the study participants, analyzed the research method and its design, population sampling, ethics in research, instruments of collecting data, techniques of collecting data, analysis of the data, the question of reliability and validity, and finally, the transition summary. In section 3, I provided the study overview, presented the findings, applied the findings to professional practice, covered the social change implications, provided recommendations for action, provided recommendations for further study, offered reflections, and finally summarized and included the conclusion study.

Section 3: Application to Professional Practice and Implications for Change

Overview of Study

In this qualitative multiple case study, I sought to investigate the strategies that ISSMs employ in nonprofit organizations to protect against cyberattacks. The research population comprised five IT managers and directors working in nonprofit organizations with the following characteristics: (a) licensed to operate legally in the state of Maryland, the District of Columbia, and Virginia; (b) employed at least 150 personnel; (c) implemented cybersecurity measures effectively, and (d) recorded at least $5 million in annual gross revenue. The study was based on the GST as the conceptual framework. During the interview session and the review of archival company documentation, participants' responses contributed to all the data to address the research question. The major themes that resulted from the data collected were (a) cybersecurity strategy, (b) cybersecurity awareness, and (c) dependence on third-party infrastructure services vendors. In my analysis of the study's findings I sought to determine the leading strategies that ISSMs in nonprofit organizations employ in protecting against cyberattacks.

Presentation of the Findings

I intended this study's primary research question to determine the strategies ISSMs at nonprofit organizations employ to protect against cyberattacks. I used open-ended semistructured interview questions (Appendix) and archival documents to gather data for the study. I determined the attainment of data saturation when the interview respondent data and the archival company documents became repetitive. As the researcher and the primary data collection instrument, I created a database and kept an audit trail of the participants' correspondence and archival documentation. I used QSR International NVivo to analyze the research data. I imported all the responses collected during the interview sessions, interview notes, archival company documentation, and the member-checked interpretive files.

The analysis of the archival documents of nonprofit organizations, including organizational policies and business reports, corroborated participants' interview responses. I used pseudonyms for each participant as P1, P2, P3, P4, and P5. Participant 1 came from Organization 1, while participant P2 was from Organization 2, Participant 3 from Organization 3, Participant 4 from Organization 4, and Participant 5 from Organization 5. The three themes that emerged from the analysis were: (a) cybersecurity awareness, (b) cybersecurity strategy, and (c) dependence on the third party. Table 1 illustrates the three major themes and the respective references.

Table 1

Themes and Their Respective References

Major themes	Participants	Response (%)	Documents	References
Cybersecurity awareness	5	100	30	68
Cybersecurity strategy	5	100	25	44
Dependent on the third party	5	100	8	52

Note. References depict the frequency with which participants mentioned the themes.

Theme 1: Cyber Security Awareness

The relevant subthemes under cybersecurity awareness are data breach, understanding protection, understanding strategic plans, and understanding third-party vendors. Table 2 highlights the subthemes under the cybersecurity awareness theme.

Table 2

Subthemes Under the Cybersecurity Awareness Theme

	Participants		Documents	
Major/minor themes	Count	References	Count	References
Data breach	5	17	3	7
Understanding protection	5	17	9	14
Understanding strategic plans	5	12	10	27
Understanding third-party vendors	5	13	8	16

Data Breach

Data breach refers to the unauthorized access to confidential data, such as customer data, for purposes of exploiting it (Kude et al., 2017). Perpetrators of data breaches may be internal players in the organization, such as employees, or external players such as hackers. Based on the participants' responses, organizations must establish practical strategies for protecting against data breaches. Three archival documents used in the study underscored the significance of using unique strategies to address data breaches in the organization. P1 indicated that they address data breaches in the organization by scanning emails and avoiding responding to those emails. A policy document from Organization 1 highlighted that "The organization has an established Data Breach Team led by the IT director, with the mandate of making all-time critical decisions about the management and containment of data breach incident." Based on P1's response and the evidence presented in the organization's policy document, it is evident that the organization understands how dangerous data breaches can be in perpetrating information loss and exploitation, hence the need to scan the emails and have a data breach team ready to ensure they are safe.

P3 said, "We have a security team which is headed by one of our partners, and she's responsible for at least keeping track of our security posture. We don't have like a centralized place that we like to watch all our infrastructure traffic." From P3's response, the organization's clear strategy relies on a security team responsible for continually assessing its security stance to control or avert data breaches. For P4, their approach entailed hiring an external company that carries out audits and risk assessments on their behalf. Based on the audit and assessment results, the company determines its performance regarding the data breaches involved. A policy document from Organization 4 indicated that the organization would collaborate with external expert IT firms to identify potential data breach loopholes within the organization's systems and act decisively towards stopping the breach.

P5 continued,

> We look at the audit log, we look at the security event, we look at the security log, we look at strange IP addresses coming from wireless devices, we look at the time of the day, and we look at all the suspicious activities that are going on at a certain period.

A privacy and safety policy document from Organization 5 indicated, “A Data Leakage Prevention (DLP) software should be used at all times to help the organization put data breach in check at all times.” P5’s response, together with the archival document evidence, reveals that the organization uses various vital indicators to keep data breaches in check at all times.

The participants’ responses underscored Daniel Ani et al.’s (2016) observations that **u**nderstanding and controlling data breaches is a critical aspect of cybersecurity awareness in any organization. The participants' responses further enforced Gordon et al.’s (2015) view that nonprofit organizations, just like for-profit organizations, must govern their data to guarantee sufficient cybersecurity awareness. Once a nonprofit organization enhances its internal capabilities to protect and ensure high-quality data through the data lifecycle, it achieves data security, data integrity, consistency, and availability (Daniel Ani et al., 2016).

The data from participants’ responses and supporting literature aligned with the concept of GST in terms of proposing better organizational systems that enhance efficiency. Based on Chen et al.’s (2012) description of GST, systems can cooperatively interact and relate to form a superior system that will prove challenging to be manipulated easily by hackers. According to Gordon et al. (2015), cybersecurity breaches mainly result from a lack of information system awareness, causing employees to blunder in sharing their login details, sending classified information to the unintended recipients, and so forth. The responses by P1, for instance, showed evidence of an established system in the organization used holistically to track and remove harmful emails that may cause a data breach.

Understanding Protection

Understanding protection in terms of cybersecurity awareness means acknowledging the significance of guarding data within the organization. During the interviews, three of the participants mentioned efforts undertaken in their respective organizations to protect stored data. P1 stated, “We are trying to work on as well as like protecting our data and protecting our organization.” An organizational document from Organization 1 mentioned that “all data repositories within the organization have controlled access that allows only those with the right credentials to access it.” This response, together with the documentary evidence, acknowledged efforts in the organization to protect organizational data because data is a critical resource requiring total protection at all times to ward off hackers. Understanding protection is an essential aspect of cybersecurity awareness. An ISSM in a nonprofit ought to assess and determine whether the risk that comes with outsourcing the organization’s security protection operations to a third-party entity outweighs the organizational losses. Similarly, P4 said, “Our management has been cooperating with us to give us enough resources to protect the organization.” An official document from Organization 4 read in part, “The data manager must ensure that the system in the organization, including computers, databases, and removable data storage options, has the full capability to ensure data integrity.” Based on P4’s response and the details of Organization 4’s official document, the organization had prioritized plans to achieve data protection. The management is the top decision-making organ in most organizations, and their involvement in data protection is crucial in guaranteeing cybersecurity awareness.

P5 affirmed, “The other way that we protect our information at our disposal is we encourage employees not to create a sensitive document and leave it on the network printer where anybody can just walk in and pick it up.” A privacy and safety policy document from Organization 5 stated, “All employees must have a unique password that allows them to venture into the system and interact with the data.” In analyzing the responses and document evidence, it was clear that employees play a significant part in ensuring cybersecurity in the organization. All the organization's security rules and policies become meaningless if the employees do not take the responsibility to learn and implement them effectively. ISSMs in organizations must direct their focus on the employees to ensure that they create sufficient cybersecurity awareness. Cyberattack constitutes a significant challenge in organizations as they try to protect their data from disappearing. Several systems such as Intrusion Prevention System, Intrusion Detection System, packet shaping devices, firewalls, and so forth, are used to protect networks.

The participants’ responses highlight the significance of employees and the nonprofits as a whole understanding the essence of protection in achieving cybersecurity. According to Mierzwa and Scott (2017), most nonprofits bare the brunt of data breaches and hacker interference because of the limited funding extended towards IT development and control. The poor funding has resulted in poor protection knowledge or understanding in most of the organizations. Jagalur et al. (2018) concluded that nonprofits have limited understanding of cybersecurity because of their lack of cybersecurity specialties to take charge of their IT units. When an organization lacks proper understanding of cybersecurity, they fail to align their goals with good cybersecurity practices. Nonprofits must put more seriousness in pursuing protection understanding in the organization to enhance their protection mechanisms against data breaches and hackers (Jagalur et al., 2018). Because many nonprofits deal with personal data, they must prioritize training their staff on the necessary technical and organizational measures on security to increase their protection knowledge (Dove, 2018). Such cybersecurity protection knowledge will empower the employees to understand and implement comprehensive data security laws effectively to the advantage of the organization.

The GST concept generally captures the usefulness of protecting a system because it underscores the necessity of strategy mix towards achieving data security. Based on Bertalanffy's (1968) principle, cyberattacks constitute observable phenomena causing social problems afflicting nonprofits. Protecting organizations against the effects of cyberattacks helps achieve a metascientific foundation that is part of general systemology. Practically, many organizations establish a common policy on data safety and security instead of going with individual employee's motivation to implement information security policies (Doherty & Tajuddin, 2018). Through the training of employees on data security, organizations pro-actively implement the GST principle of protecting their systems against data exploitation (Doherty & Tajuddin, 2018). As systems, organizations must establish the necessary infrastructure and adopt a material culture enforcing protection behavior among their employees (Kim & Kim, 2017).

Because cybersecurity is a dynamic situation, nonprofits must continually think of establishing protection systems to encourage the employees to put in voluntary efforts.

Moreover, organizations can also rely on different attack modeling techniques to support their understanding of the attack. Organizations must prioritize the protection of their network from attackers. The findings of this research further support the GST concept, especially its system technology aspect. Creating knowledge and awareness about data protection helps organizations to protect their valuable data because it creates harmony between the policies, software, hardware, and training (Carrapico & Farrand, 2017).

Understanding Strategic Plans

Understanding strategic plans for cybersecurity awareness increases the interpretation by stakeholders in the organization regarding the tactical moves to implement to fulfill cybersecurity awareness. Participant P2 indicated how understanding strategic plans help in establishing cybersecurity awareness. In particular, participant P2 said, “The success of any cybersecurity program is what we call a strategic cybersecurity plan. Some people might call it a cybersecurity margin plan or system security management plan, but the keyword there is strategy.” Similarly, the policy document from Organization 2 read in part, “Efforts to protect data must start with information creation, with the main focus being the definition and documentation of access control decisions and protection levels. Protection should be enforced throughout the data life cycle.” From P2’s comprehensive response, no cybersecurity plan is useful to the organization unless a strategic plan is established. The strategic plan enables a better understanding of the environment and profile, empowering the employee to know its inadequacies and vulnerabilities. Without a strategic plan, the ISSM cannot make the needed modifications to attain the results desired.

The response above underscores the help strategic cybersecurity planning achieves towards the organizations' tactical aims and capabilities. Efthymiopoulos (2019) strongly espoused the significance of cybersecurity planning in achieving tactical aims and capabilities because it achieves a policy framework, methodology outline, orientation, and implementation for all matters about the internet when interconnected. The response also illustrates how strategic plans play a significant role in enhancing cybersecurity awareness within organizations. According to Efthymiopoulos (2019), knowledge of strategic plans helps in projecting the criticality of cyber-security in terms of policy. When employees in a nonprofit understand cybersecurity strategic plans, they also appreciate the importance of enhanced methods for the organization’s cyber-dimensional operations. The organization will benefit from numerous cybersecurity elements and variables, resulting in a grander cybersecurity strategy. Junior & Santos (2016) also believed that an organization’s information security strategic plan positions it to lessen, shift, accept, or evade information risk associated with people, technologies, and processes. The cybersecurity plan produces proposals emphasizing the need to establish a joined cybersecurity approach.

The strategic cybersecurity plan also aligns with GST. Based on Von Bertalanffy’s (1972) GST concept, the external environment lies outside an organization's control because of many irregular forces such as technology or innovation, competition, and others' economy. These factors or forces make up sub-systems that constitute a more extensive system. GST's explanation of the strategic planning model, therefore, appreciates how each of the sub-systems interacts. By using the GST conceptual approach, the ISSMs learn more deeply about the technological and innovation trends and the decisive nature of the interaction between these diverse components.

Understanding Third-Party Vendors

Third-party vendors are external actors who offer IT services that the organization may not fully provide from its internal IT department. Understanding third-party vendors are critical in the cybersecurity awareness quest because it enables the organization to determine its capacity to align with its anticipations. Three of the participants illustrated their understanding of third-party vendors and their significance towards achieving cybersecurity awareness in the organization. For example, participant P1 opined that third-party vendors have a more profound knowledge of cybersecurity, which helps them advise client organizations whenever security issues occur. This response proves the extent to which organization managers trust third-party vendors based on the knowledge they possess. The analyzed safety and privacy policy document from Organization 1 illustrated that the organization would incorporate third-party vendors' expertise towards delivering what the organization cannot deliver. Participant P4, on the other hand, affirmed that their capacity to handle their in-house cybersecurity was limited as an organization. Therefore, the organization understands the necessity of outsourcing third party vendors with higher capabilities and experience to guarantee cybersecurity awareness among the employees.

Similarly, participant P5 explained that the organization works with an elaborate third-party system they trust to address some of their internal issues that touch on cybersecurity. The trust of the third-party vendor system is based on the vendors' expertise in handling cybersecurity. An official document from Organization 5 analyzed in this research explained that the organization would procure third-party vendor services if they proved to be value for money and technically superior to what the organization provides internally.

These responses by research participants echo Jagalur et al. (2018) position that many nonprofit organizations acknowledge they lack the optimum capacity to secure their IT infrastructure and services. The responses also affirm Bauer et al. (2017) observation that most nonprofit organizations have incorporated security procedures and policies that integrate third party operations. Generally, as Bauer et al. (2017) further added, trusted third-party providers, limited liability, risk reduction, and vendor training constitute critical intervention measures that nonprofits’ ISSMs use when incorporating third-party vendors' security management. However, a nonprofit organization must understand the roles and capacities of a third-party vendor before opting to incorporate its assistance in enhancing cybersecurity awareness.

The system philosophy aspect of the GST aligns with the discussion about nonprofit organizations integrating third-party vendors in their cybersecurity awareness quest. Many nonprofit organizations invest very little towards their basic computer systems, leaving their systems widely exposed to hackers who use superior skills and technology. Based on the GST concept, the nonprofits rely on third-party vendors' input to strengthen their systems and enhance efficiency. According to the GST foundational theory, organizations can establish superior systems protected from hackers using numerous sub-systems sourced from competent third-party vendors.

Theme 2: Cybersecurity Strategy

The cybersecurity strategy theme includes some basic subthemes: acquisition, auditing, awareness, security plan, security procedures, and training. Cybersecurity strategy refers to the overall plan of actions intended to achieve improved organizational infrastructure resilience as far as IT security is concerned (Pardini et al., 2017). A highly functional cybersecurity strategy must constitute a high-level approach that identifies a range of organizational objectives and priorities for achievement within a specified period (Bauer et al., 2017). Table 3 highlights the subthemes under the cybersecurity strategy theme.

Table 3

Subthemes Under the Cybersecurity Strategy Theme

	Participants		Documents	
Major/minor themes	Count	References	Count	References
Acquisition	5	19	1	6
Auditing	5	24	3	13
Awareness	5	12	3	19
Security plan	5	7	7	10
Security procedures	5	65	5	12
Training	5	28	6	42

Acquisition

Acquisition refers to the procurement of the requisite IT tools and strategies for ensuring cybersecurity. Based on the participants' responses, budgeting is essential in acquiring cybersecurity strategies in nonprofit organizations. One archival document in the study directly addressed budgeting, which was significant for the findings. P1 stated, “We come up with a budget based on the data growth from previous years, and based on that, we try to come up with several what we think we’ll need.” The archival document from Organization 1 stated in part, “The IT director is in charge of the cybersecurity budgeting process, ensuring that the company gets value for money in all cybersecurity tools acquired.” The evidence highlighted by P1 and corroborated by the archival document illustrates how the organization prioritizes the budgeting process before acquiring the desired cybersecurity strategy.

P2 mentioned that as an organization, they often evaluate their capabilities regarding the tools they own. The organization can plan its resources towards acquiring the appropriate tools based on the challenges experienced previously from such an evaluation. Based on P2’s response, it is clear that the organization aligns its cybersecurity acquisition with the resources at its disposal to avoid a scenario where it overspends its resources. On the other hand, P3 said, “We come up with a budget of what we think we will need, like increasing the storage for our data center or maybe getting new servers.” Based on this response by P3, the expenditure is only planned for the resources needed at a particular time and not for every other requirement. In other words, the budget on what to spend prioritizes the most pressing needs first before considering other less pressing needs. P5 explained that they usually set aside some money for the IT department to cushion against any eventualities arising from cybersecurity incidents.

According to P5’s response, this budgeting approach acknowledges that IT is a dynamic area that requires proper financial plans well ahead of any unseen eventualities.

These responses from research participants confirm Fielder et al. (2016) position that as a process, acquisition forms a fundamental component of cybersecurity strategy because organizations must procure all the necessary technology and assets that will aid the actualization of their strategy. For example, cloud resources can form part of the core assets that a nonprofit organization depends upon to facilitate its cybersecurity strategy (Bildosola et al., 2015). Procuring such cloud resources is necessary to ensure that the nonprofit organization's cybersecurity strategy becomes a reality. Acquisition plans should reflect in the organization’s budgeting process as the first step to ensure an effective balancing of resources (Fielder et al., 2016). Not-for-profit organizations may lack the adequate financial capability to own the most effective cybersecurity assets that guarantee a more reliable strategy because of relying on donations and grants (Jagalur et al., 2018). Budgeting helps plan the limited resources' expenditure by ensuring the prioritization of the most necessary acquisitions (Fielder et al., 2016).

The participants' responses and the evidence from the various archival documents align with GST's concept, which seeks to identify with the wholeness of both scientific and social problems (Bridgen, 2017). Data security and safety are scientific and social challenges, which can be handled effectively by incorporating scientific education. When non-profits plan their resources to procure the requisite IT tools and strategies to guarantee their data and information safety, they establish a general systemology that eventually incorporates scientific education (Drack & Pouvreau, 2015). Essentially, the acquisition is a crucial method that aims to approach the nonphysical areas of science. Thus, the GST concept helps to explain how acquiring the appropriate IT tools and strategies against data theft draws us closer to the unity of science's objective, as it develops on principles running 'vertically' throughout the universe of the separate sciences (Bertalanffy, 1968).

Auditing

Auditing refers to evaluating the effectiveness of the cybersecurity measures put in place to ensure maximum results. According to Alkalbani et al. (2017), an organization may not determine its cybersecurity strategies' effectiveness unless they measure the extent of compliance concerning data protection. The participants' responses on the question of auditing brought out its importance in the whole subject matter of cybersecurity. Three archival documents assessed by the researcher further highlighted the significance of cybersecurity auditing in different ways. P2 stated, “We evaluate the employees and see what areas require training them.” The archival document attributed to Organization 2 read in part, “Regular operational, procedure and safety audits assist in ensuring that proper controls are adequate at guaranteeing information confidentiality, shielding Personally Identifiable Information (PII), safeguarding system availability, and promoting a higher data integrity degree.” From P2’s response and Organization 2’s archival data, the company understands the critical role that auditing plays in upholding cybersecurity. The organization has stopped with regular operational audits and audits of their employees to determine the right training programs.

P1 underscored the importance of cybersecurity auditing by stating, “We hire an outside company to come and run an audit on our information system to ensure that we have everything in place.” An archival document from Organization 1 corroborated P1’s response in a section of its content which stated, “A yearly cybersecurity audit by a neutral third party will be conducted as shall be determined by the relevant authority in the organization to certify that all the necessary security guidelines are adhered to fully.” The response by P1 and the evidence adduced in the archival document clearly illustrate that the organization undertakes regular cybersecurity audits through a third-party entity. P4 added that their organization outsources auditing services from external companies, which helps them assess the risk and identify their success rate as far as cybersecurity performance is concerned. For P4, the thoroughness and professionalism of the external companies' audits give a more accurate picture of the organization’s stance regarding their cybersecurity strategies. P3 stated, “We manipulate and check audit passwords and anything important.” An archival document from Organization 3 indicated that the company does not wait until they experience an attack. Instead, it proactively carries out cybersecurity audits to establish a security baseline to ascertain the auditor's professional advice. According to P2’s explanations and even the archival document from Organization 2 referenced, auditing the system through deliberate in-house manipulations helps determine potential weaknesses that may require urgent action in making amends.

The research participants' responses affirm Alkalbani et al. (2017) reasoning that indeed organizations should embark on determining the effectiveness of their cybersecurity strategies if they genuinely seek to know their level of compliance regarding data protection. Moreover, these responses by the research participants underscore Moskal et al. (2018) observation that organizations must always have existing processes that offer guidance towards improvement and governance procedures, which in turn guarantee continuous confidence within the controls. In the same stance, Libicki (2017b) position about nonprofit organizations needing a hands-on monitoring and response system to ensure real-time response mechanism to breaches further relates perfectly with the participants' responses. As the nonprofits plan the auditing of their systems to protect against breaches, they must establish controls, processes, and technology to offer the much-needed protection. However, as Cobb et al. (2018) rightly pointed out, these anti-breach controls, procedures, and technology are not enough to ensure total safety. The nonprofit's ISSMs must ensure that they continuously assess all anti-breach systems and technology to ensure full functionality.

The GST concept constitutes a system philosophy aspect, which effectively aligns with auditing cybersecurity strategies to ensure optimal results. Cyberattacks are incredibly involved in the sense that some of the strategies devised to protect organizations eventually lose their vibrancy over time (Oakley, 2019). By continuously evaluating these intervention methods' efficacy, the nonprofits increasingly enhance their safety because they can determine the most efficient intervention methods (Cobb et al., 2018). Based on the GST concept, the nonprofits use third-party companies for auditing their systems and determining their efficacy. The GST foundational theory's principles provide room for organizations to audit their systems through sub-systems offered by third-party systems such as external vendors (Atoum & Otoom, 2016).

Awareness

Awareness of cybersecurity as a subtheme of this research signifies understanding or knowledge about the concept of cybersecurity and the basic strategies used to enhance data safety and protection. Generally, cybersecurity awareness forms one of the most critical components of data safety (Bauer et al., 2017). Employees make up the band of IT users in an organization, meaning that their understanding of cybersecurity, in general, would help quite significantly in guaranteeing data safety and protection (Bauer et al., 2017). Based on the participants' responses, it is clear that cybersecurity awareness has positive implications for an organization's cybersecurity status. Three archival documents provided the researcher with additional details to conduct research analysis regarding cybersecurity awareness. P1 said that it is always essential for the employees to discover and understand their happenings, especially concerning technologies, because this would incorporate their assistance in ensuring cybersecurity safety. The archival document from Organization 1 stated, "As members of the organization, all staff members are accountable, and have the mandate to show an understanding of their exceptional responsibility, as part of the defense to safeguard the organization's data, information, and reputation." Analyzing the response from P1 and the contents of the archival document from Organization 1, it is clear that the organization expects its employees to have cybersecurity knowledge and use the same knowledge to ensure data protection.

According to P4, apart from employees' scheduled training, their organization organizes security awareness training four times a year, whose intention is to empower the employees to fight cyberattacks. The archival document from Organization 4 stated, “Staff will be sufficiently trained on regular intervals to empower them to protect the organization’s data and information against hackers and other malicious actors.” Reviewing P4’s response and the archival document from Organization 4 informs the fact that the organization achieves cybersecurity awareness mainly by training the employees regularly. P5 stated that they even organize mock attacks without the employees' knowledge and check to gauge their awareness levels. The archival document from Organization 5 read, “As part of our proactive policy on cybersecurity, the information security manager will occasionally carry out mock attacks to test the effectiveness of data protection mechanisms.” Based on P5’s response and the archival data from Organization 5, they strictly focus on employee awareness through manipulated attacks to ascertain the level of their preparedness against real attacks.

The research participants’ responses above and the various documented pieces of evidence espouse Bauer et al.’s (2017) conclusion that creating cybersecurity awareness in the organization is the best way that nonprofits can motivate employee behavior to curb data breaches. In reality, most nonprofits put little effort to establish effective cybersecurity strategies because they consider it a costly operation compared to their lean budgets. Bauer et al. (2017) exposed this reality by noting that many nonprofits lack adequate financial resources to procure the vital IT skills and infrastructure for their use. However, as Bauer et al. (2017) noted, the lack of proper cybersecurity skills in the organization exposes it to significant data breaches and threats. Nonprofits must maintain a dedicated IT staff for long to create a wealth of experience and skills that will achieve the requisite internal awareness cybersecurity. According to McMahon et al (2015) nonprofits’ failure to maintain dedicated IT staffs denies the organization the necessary awareness that would enhance protection against hackers and data breaches in general. The lack of awareness in nonprofits has further resulted in the common use of open-source software to save costs. According to Bauer et al. (2017), using the open-source software increases vulnerability to cyberattacks unlike using proprietary software versions.

The responses and archival document evidence further echo Almubark et al. (2016) observation that creating awareness is an effective strategy that works by creating an influential security culture, which always keeps the employees updated about the technology, including enabling them to understand the processes as well as other organizational factors that touch on data security.

Based on the participants' responses and supporting documents, cybersecurity awareness is strongly linked to GST as it ensures a practical system against data theft or manipulation. In particular, GST considers an organization as an open system in constant interaction with its local environment through the exchange of ‘materials’ (Schneider et al., 2016). Essentially, when organizations create strong cybersecurity awareness among the employees, they pursue a mechanism intended to continually secure the organization even as it continuously interacts with its local environment. Cyberattacks increase when the organization fails to streamline and harmonize its policies, software, hardware, and training.

Security Plan

A security plan refers to an organization's comprehensive strategy to shield its customers, employees, and corporate information against compromise. Participants responded by describing some of their organizations' security plans, pointing out their importance regarding cybersecurity strategy. Seven archival documents analyzed by the researcher provided the additional ground to elaborate on the essence of cybersecurity plans in general. P1 said, “We need to invest a lot more into the data security in terms of having more tools at our disposal to remain a little bit more proactive. We use our antivirus system and intrusion protection system to ensure that we are always ready to face any sort of data breach or attack.” The archival document from Organization 1 stated, “The IT Manager determines the adoption of anti-virus software and supplementary malware protection tools to detect, prevent, deter, and alleviate the introduction and exposure of viruses/malware on the computer devices and networks within the organization.” The response from P1 and the archival document from Organization 1 highlights antiviruses and other related tools such as intrusion protection systems as part of the security plans against cyberattacks.

P2 said, “Access control is a big one, and we’re there talking about authentication for every individual touching any system and any information resources. Employees in remote environments require two-factor authentication.” This response by P2 identifies how organizations are limiting access to their systems and data networks as a strategy to limit compromise by hackers and other unauthorized people. P3 described the security plans in their organization, focusing more on individuals because each employee covers a specific security aspect in their niche areas. The organization lacks centralized control and instead relies on the employees as its primary security plan. The archival data from P3 stated, “This policy approves cloud services to necessitate file sharing and storing 1) with vendors providing suitable protection and recovery for the organization’s information, and 2) with clear restrictions about the storage of the organization’s protected information.” Based on P3’s responses and the archival document from Organization 3, organizations resort to storing data externally as part of their security plans to safeguard against data losses and compromise.

P4 talked about a security plan in which a third-party company collects all data in digital format and sanitizes it to ensure proper and periodic standardization of everything. Archival document from Organization 4 stated, “The organization will provide all staff members access to Microsoft Office 365 and Google Apps. The staff members will access Microsoft “OneDrive for Business” and "Google Drive" using accounts created on their login ID.” The response by P4 and the evidence contained in the archival document for Organization 4 equally shows how organizations are resorting to third-party players as part of their data security plans.

These research participants' responses align with Martin and Murphy’s (2017) observations that organizations need to build adequate capacity in advance to guard their sensitive information. Nonprofits may find data privacy more challenging to implement because of the fluidity of the concept compared to their fringe capacities, but reality points to the need for organizations protecting their data and IT infrastructure against compromise from hackers. According to Adams (2017), planning for data security helps the nonprofits to clearly define data privacy and effectively establish mechanisms to address it. The cybersecurity planning that includes antivirus systems, intrusion protection strategies, and cloud computing constitute better organizational systems underscored by GST (Zhang et al., 2019). In particular, nonprofits must endeavor to build a safeguard mechanism for their data and IT assets well in advance to ensure proactivity when it comes to protecting sensitive data at their disposal (Abouelmehdi et al., 2017). Data security planning at the nonprofits level, according to Adams (2017), targets the entrenchment of storage and the processes of transportation within security measures.

Generally, the research participants' responses and document evidence drawn from the organizations underscored the link between cybersecurity planning and the GST concept. According to Proctor and Xiong (2018), GST's principles are linked to Cybernetics principles in the sense that everything beginning from neurophysiological systems to societal activities can be made into structured control systems constituting feedforward and feedback loops. When organizations plan for cybersecurity, they strategize through scientific inferences abstracting human decision making based on controlled experiment findings (Proctor & Xiong, 2018). Many organizations face technological advancement pressure in a system where human lives are increasingly intertwined with the cyber environment. Because of the increased interaction, organizations find it necessary to pursue cognitive psychology and interdisciplinary research as part of their security planning (Proctor & Xiong, 2018). The complex nature of cyberattacks require a different approach to security defenses. The dynamic new generation threats are evasive, resilient and complex, requiring proper planning to combat the threats. Nonprofits must gather and share real-time information on cyber threat to convert it to accurate threat intelligence to either prevent attacks or implement timely disaster recovery. Thus, the link between cybersecurity planning and GST provides the tools that focus on tackling the cyber cycle (De Boer & Andersen, 2016). According to Fal (2016), security planning in cybersecurity is a form of closed-loop feedback mechanisms with output that links directly with the subsequent system's input. GST constitutes feedback loops utilizing behavioral relations (Drack & Pouvreau, 2015).

Security Procedures

Security procedures refer to the set of rules that an organization establishes about practicing responsible security to guide employees, partners, board members, consultants, and other end-users accessing internet resources and online applications, sending data over networks. Based on the participants' responses, security procedures exist in their organizations as part of their elaborate cybersecurity strategy. Five archival documents were available during this research’s analysis. As standard practice, most organizations adhere to a set of security practices and processes to ensure that their data remains safe at all times (Gordon et al., 2015). P5 noted, “One of the procedures that we use includes access control, where we make sure that access to the system remains restricted to the people supposed to use the assets.” An archival document from Organization 5 stated, “Group IDs shall not generally be allowed as access means to the organization’s data, but might be approved under exceptional situations if other adequate access controls are in place.” This response by P5 and the corroborating evidence from the archival document from Organization 5 identify how organizations are settling on the use of access control as part of their cybersecurity procedures.

P1 stated that part of their procedures included using an antivirus system, an intrusion protection system, and a requirement for users to change their password every 60 days. Users are also required to use a complex password containing special characters, numbers, and lower uppercuts. An archival document from Organization 1 stated, “Users shall get trained on password protection, with the password policy implemented to confirm that users change their passwords after every 60 days or as shall be determined by the information security manager.” The evidence as noted in P1’s response and Organization 1’s archival document reveal that organizations may use a combination of strategies, including strict password policies, antivirus systems, and intrusion protection mechanisms, as part of their cybersecurity procedures. P2 added, “To access the system, some can only read all the information while others can only read some of the information. Some can read and write to the system and even change the data in the system, which are all part of our security procedures.” The archival document from Organization 2 stated, “Employees can only access information necessary for the effective performance of their respective job duties. Access will be based on an employee’s responsibility or job competency, with their access to data resources limited to either viewing, creating, or modifying files.” The response from P2 and the details in the archival document from Organization 2 points to the fact that role-based access control is among the cybersecurity procedures that organizations use to protect their data from compromise and theft.

P3 explained that the organization has a sensitivity setting, which protects sensitive information sent via the internet with such features as one-week password expiration. Such sensitive information automatically deletes itself if the password expires within the stipulated period. The archival data attributed to Organization 3 recorded, “Sensitive data will automatically delete from the storage or computer device containing it immediately after the password used to protect it expires.” Basing on this response by P3 and the archival data evidence, it is clear that organizations are using automatic systems that can self-delete any data considered sensitive to protect it from hackers and other malicious actors. P4 answered that their organization's security procedures range from implementing a group policy to software called server apps that manage privileged users and track endpoint devices. The response by P4 underscores the use of privileged user accounts by organizations as part of their cybersecurity procedures that only allow specialized levels of access based on elevated permission levels.

These responses by research participants underscore Gordon et al., (2015) position that, generally, many organizations adhere to the standard practice of observing security practices and processes as a means of guaranteeing safety at all times. Similarly, the responses echo Bauer et al.'s (2017) findings, which posited that nonprofits engage in numerous security procedures such as creating awareness about information systems through special programs implemented by IS managers. Almubark et al. (2016) observed that nonprofits' need to create an influential security culture as part of their security procedure is equally in tandem with the research participants' responses. According to Almubark et al., such a security culture in the nonprofit can achieve the intended purpose by motivating the employee behavior towards curbing data breaches. Similarly, the research participants' responses validate Zafar et al. (2016) that organizations need to rally support the top management for IT governance practices to ensure adequate security procedures.

In general, the concept of security procedures in nonprofits ties with the system philosophy espoused by GST. In particular, the system philosophy aims to develop new thinking or viewpoint based on systems concepts. Thus, nonprofits comprise open systems characterized by contingencies that face significant consequences when faced with data breaches (Caws, 2015). The nonprofits' main components of a system are the inputs, outputs, processes, subsystems, and feedback. By establishing effective security procedures, the nonprofits can identify cybersecurity breaches' symptoms and describe them independently and how they interrelate to help understand how the organization can prevent them (Rousseau, 2015).

Training

Training refers to the intentional teaching of individuals in the organization to impart skills that would empower their data and information protection efforts. The responses by participants touched on training about their respective cybersecurity strategies. Additionally, the archival documents accessed by the researcher corroborated the responses by the participants quite spectacularly. Training employees on cybersecurity imparts skills in improving the organization's overall security, reducing avoidable errors that may cause data losses and breaches, enhancing company reputation, and bolsters employee confidence (Almubark et al., 2016). When employees receive adequate cybersecurity and safety training, the organization increases its productivity and minimizes its operation costs (He & Zhang, 2019). P1 said, “We make sure to educate our users on what they should be doing." The policy document from Organization 1 stated, "All employees in the organization with access to the Information Resources must undertake security awareness training in their first 30 days after being hired." Based on the response by P1 and the policy document from Organization 1, it is evident that organizations use mandatory cybersecurity training as part of their strategies to equip their staff with knowledge on data protection and safety.

P2 responded, "We have training sessions with the users where they can ask questions." Based on this response by P2, it is evident that organizations emphasize the need to train their employees regularly to build a significant internal knowledge base that would help guard against data theft and compromise. P3 stated, "We train our employees. Training is important, and it does not have to be formal because we have experts who do this day-to-day. It could be a simple thing as a 15–20-minute conversation." The policy document from Organization 4 stated, "The organization shall continuously evaluate the cybersecurity skills held by all the employees, and promote regular training to address any potential skill-gaps." Analyzing the response by P3 and the details in the archival document from Organization 4 reveals how organizations invest more time and resources to invest in training programs to address cybersecurity threats effectively. P4 explained that their organization uses two strategies: sending the employees to training and conducting in-house training for people in the IT security department. According to P4, external training happens at least once every month, where an individual in the team receives the necessary skills. Based on the response by P4, organizations also adopt a mix of training methodologies to ensure that their cybersecurity strategies are convincing enough.

Building a strong data security culture serves as an appropriate approach that nonprofits can adopt to effectively achieve cybersecurity (Zafar et al. 2016). Training the employees about cybersecurity eventually uses special programs entailing systematic planned interventions that uninterruptedly inform the employees and stakeholders about the security information (Bauer et al., 2017). The training creates culture awareness through motivating the employees to develop behaviors to curb data breaches (Almubark et al., (2016). Training is an effective strategy for creating an influential security culture because it ensures the employees are continually updated about the technology. Training also enables the employees to understand the organizational factors and other important processes regarding data security (Almubark et al., 2016). According to Zafar et al., training the employees does not only build a compelling data security culture, but also enhances risk management activities and security planning.

Cybersecurity training is a critical concept closely associated with GST. According to Verhoeff et al. (2018), GST consists of three aspects: systems science, systems technology, and systems philosophy. GST's main philosophy focuses on how the system works together and how one part of the system leads to understanding the other parts. As part of the organization system, employee training imparts simple mathematical ideas that fundamentally formulates feedback, equilibrium, information, stability, entropy, regulation, constraints, communication, and so forth. Training serves as an input mechanism that interacts with the system through continually imparting skills that enhance employees' willingness to protect data (Doherty & Tajuddin, 2018). According to Kim and Kim (2017), the use of training as an interaction mechanism with the cybersecurity mechanism attains the appropriate compliance behavior through material culture and support infrastructure. Nonprofits have a duty of promoting compliance by integrating critical training to encourage the employees to put in voluntary efforts. When nonprofits train their employees to enhance their cybersecurity knowledge, they enable them to achieve better knowledge regarding systems science, systems technology, and systems philosophy, all of which combine to ensure a safe organization in terms of data security.

Theme 3: Dependence on Third Party

The subthemes under this theme include expert technical support, limiting nonprofit liabilities, and limiting risk exposure. Integrating third party support is an effective way of implementing cybersecurity, especially for nonprofit organizations lacking critical in-house IT expertise (Rossouw & Willett, 2017). Table 4 highlights the subthemes under the dependence on third-party themes.

Table 4

Subthemes Under the Dependence on the Third Party

	Participants		Documents	
Major/minor themes	Count	References	Count	References
Expert technical support	5	20	4	13
Limiting non-profit liabilities	5	3	2	9
Limiting risk exposure	5	5	2	3

Expert technical Support

Expert technical support refers to the standby help or assistance that cybersecurity specialists often avail to users of computer systems and data networks to reinforce their efforts against data threats and risks. Mostly, third-party IT companies lend their technical support that often benefits client organizations lacking the same capacity level (Jagalur et al., 2018). The operational efficiency of third-party IT companies guarantees the client organizations absolute cost benefit because of their experienced workforce, elaborate hardware, and software resources built over time (Gordon, Loeb, et al., 2015). Participants' responses identified their organization's dependence on third-party IT service providers for technical support reasons. Similarly, archival documents assessed in this study underscored third-party vendors' significance in offering technical cybersecurity support. P4 posited, "The vendor does what they do all day long because they are specialized, have the skill, and have the resources to protect." The policy document from Organization 4 indicated that the organization would procure third-party IT specialists and vendors whenever necessary to offer technical support as would be determined. An analysis of the above response by P4 and the content in the policy document shows that organizations often rely on third-party IT companies for expert technical support to enforce their safety mechanisms against data loss and compromise.

P2 stated that they had entrusted a cloud service provider to manage all operations on their behalf to concentrate their clients' activities. The archival document from Organization 2 stated, "The external cloud service provider must extend support services to users whenever required." Based on the response by P2 and the evidence contained in the archival data from Organization 2, it is deducible that organizations using cloud services also get technical support that helps in their quest to ensure the safety of their data and information. P5 explained that their organization depends on a vendor system that handles all their IT needs they consider too technical to handle. The response by P5 highlights the fact that organizations receive a mix of technical support from external service providers to bridge their lack of cybersecurity inadequacies.

These research participants' responses tie with Bauer et al. (2017) findings that most nonprofits have incorporated numerous security procedures that entail integrating third-party operations. Given the limited IT and skill capacity in most nonprofits, the option of procuring technical support from third party service providers ensures effective cybersecurity performance (Jagalur et al., 2018). According to Gordon et al. (2015), third-party IT service providers guarantee client organizations operational efficiency in terms of cost and performance quality. The expert technical support from the third-party players guarantees effective workmanship, high-level software resources, and elaborate hardware acquired over time (Gordon, Loeb, et al., 2015). The research participants' responses further encompass Bauer et al.'s belabored point that trusted third-party providers make up critical intervention measures suitable for nonprofits' ISSMs for security management. Nonetheless, nonprofit organizations need to understand the roles and capacities attributed to specific third-party vendors before engaging their services to pursue expert technical support.

Expert technical support constitutes an essential aspect of GST. According to Ludwig von Bertalanffy (1968), a system achieves wholesome functioning when its parts successfully interdepend on each other. A salient characteristic of this definition is the interrelatedness of parts within a system. Thus, in an organizational context, expert technical support may be considered an important part of achieving the organization's wholesome functioning (Bridgen, 2017). The major process that characterizes how components relate in a system is the homeostatic propensity that smoothens or balances operations. The expert technical support within the organization helps in the smoothening of operations, which guarantees the proper functioning of the organization as a whole.

Limiting Nonprofit Liabilities

Based on the data analysis, nonprofit organizations consider limiting their nonprofit liabilities because they often operate on limited financial resources that hinder their full potential ability. Limiting nonprofit liabilities refers to organizations' practice to minimize the obligation of data losses and compromise by hackers (Jagalur et al., 2018). P1’s response captured the same sentiments and automated specific jobs to prevent data breaches. An archival document from Organization 1 corroborated P1’s response stating that operations automation at various levels will be prioritized to limit human interaction, increasing data loss risk. P3 implied that their organization has limited liabilities by contracting out data destruction services to a third-party firm that efficiently does it because it is their primary business area. Based on P3’s response, organizations lacking internal capacity often procure third-party specialist firms to handle delicate operations likely to result in data losses if they were to be handled internally. P4, on the other hand, stated, “We carry out regular vulnerability tests on our data systems to ensure we eliminate probable weaknesses. The tests are wide-ranging, from evaluating password strengths and effectiveness to assessing DDoS attack remedies implemented.”

Based on the research participants' responses, there is a connection between the ideas mentioned and the literature by Alshahrani and Traore (2019), positing that automated security protocols implement numerous programmed security analysis mechanisms. The robustness of these automated systems can effectively help nonprofits track, detect, and eliminate cybersecurity threats compared to having manual systems handled by employees. Similarly, the participants' responses tally with Jagalur et al. (2018) findings that third-party vendors significantly cushion organizations, including nonprofits, against too costly and technical IT operations liabilities. According to Holtfreter and Harrington (2015), third party IT vendors specialize in particular IT areas, which gives them the utmost capability and potential to handle obligations that client organizations such as nonprofits may not manage efficiently. Essentially, the nonprofits transfer their obligations to a superior third-party player with adequate capacity to protect them against probable data breach liabilities.

The theoretical basis of GST aligns with the discussion regarding limiting nonprofit liabilities, as highlighted above. In particular, the organization is an open system with continuous interaction with its local environment by exchanging ‘materials’ (Schneider et al., 2016). GST is a social theory explaining the sharing of ideas, arguments, hypotheses, explanatory speculations, and thought experiments to the benefit of human societies and elements. The nonprofits represent human societies in which social interactions occur continuously to help in achieving cybersecurity. When nonprofits seek expert advice from cybersecurity experts, for instance, they acquire ideas and expertise that helps them to achieve effective cybersecurity. The social aspect of GST is useful in limiting nonprofits liabilities because it promotes the sharing of useful ideas and knowledge whose adoption and implementation guards against data exploitation. The interaction between the organization and social systems calls on the nonprofits to limit potential liabilities to guarantee superior systems protected from hackers.

Limiting Risk Exposure

Limiting risk exposure equally helps organizations succeed in managing cyber risks. Common interventions aimed at limiting risk exposure include 24-hour state-of-the-art physical security scrutiny, physical access controls, together with multiple-layered perimeter protection (Kajiyama et al., 2017). The participants' responses showed that they were aware that their nonprofits were vulnerable to cybersecurity incidences and tackled the risk by depending on vendors to supply requisite infrastructure. For example, P1 held that the organization keeps scrutiny on employees' login credentials to avert a scenario where hackers can steal such credentials and access critical organizational databases undetected. The archival document from Organization 1 indicated that employees are not allowed to recycle passwords after their expiry. Employees are also supposed to use their biometric data to limit data risk exposure as part of their login details. Based on the response by P1 and the evidence adduced by the archival document from Organization 1, it is evident that the organization is proactive in putting in place data safety and security measures in earnest.

P2 answered, "The organization has installed security cameras at all strategic locations to physically capture images and footage of any individuals, whether employees or outsiders, who may engage in any data breach activities. The archival document from

Organization 2 read in part that the organization’s premises shall remain under security camera surveillance at all times to help in detecting activities that may jeopardize its information security. P3, on the other hand, answered, “Access to the data room in the organization is physically protected by a large physical door that can only be opened using a security card issued to a few IT staff. This intervention was instituted to protect data and related systems from being compromised by intruders.” P4 indicated that apart from the organization enjoying a perimeter fence and a security guard around its premises, video surveillance offered through a network of CCTV cameras limits their security exposure quite significantly. P4’s response underscores the organization’s total focus on using physical and nonphysical interventions to limit its data exposure from exposure risks. P5 also mentioned a mechanism implemented in the organization where employees’ login credentials were closely monitored and automatically canceled after every two months to ensure that hackers who may steal them are denied access to the system.

The responses tally with Kajiyama et al. (2017) literature observations that many organizations employ 24-hour state-of-the-art physical security scrutiny, as well as physical access controls and multiple-layered perimeter protection to track hackers’ actions. Limiting risk exposure equally helps organizations succeed in managing cyber risks. Nonprofits can consider such interventions as physical access controls, multiple-layered perimeter protection, and so forth to cut down the risk exposure they face (Kajiyama et al., 2017). Nonprofits can also exploit the more robust cloud systems that focus on achieving cybersecurity through establishing on-premises infrastructure

(Rossouw & Willett, 2017). Given that most nonprofits lack adequate resources to protect their data and infrastructure against breaches, cloud systems present them with a practical alternative that guarantees data security without requiring substantial upfront investment (Attaran, 2017). Similarly, the participants' responses echo Parks et al. (2017). They hold that a mere privacy policy without instituting physical protection mechanisms can prove to be virtually meaningless and highly superficial to a nonprofit organization. Thus, ISSMs in nonprofits must endeavor to use physical barricades and other deterrence mechanisms to limit the risk of exposure to their data and data systems.

These responses by research participants and the corroborated archival documents align with the basic principle of GST. Generally, GST’s overview of a cybersecurity strategy is from a systems integration perspective, emphasizing organizations' need to implement a mix of data security strategies (Kordova et al., 2018). One security strategy that nonprofits can implement to achieve cybersecurity includes training the employees. Training is an aspect of GST that seeks to effectively educate the employees on the significance of their cybersecurity handling (Doherty & Tajuddin, 2018). Informed employees will limit the organization’s risk exposure because the training they undergo boosts their willingness to protect data. Nonprofits stand to benefit from enhanced cybersecurity protection and control if they train their employees to achieve high-level compliance behavior. When nonprofits limit their risk exposure against data loss, they enhance their willingness to take necessary steps to protect data. The nonprofits embark on promoting compliance systems to ensure protection against intrusion and theft actively.

Applications to Professional Practice

This study’s findings, the outcome of the conceptual framework’s analysis, and the scholarly literature review contribute to discussing the strategies ISSMs at nonprofits employ in protecting against cyberattacks. In particular, the study’s findings illustrate that identifying the ISSMs’ execution of the best cybersecurity practices towards protecting the organization’s is the most significant contribution. Bordoff et al. (2017) emphasized the need for the nonprofits to train their staff about security and substantiate third parties' best practices.

Based on the research study's outcome, my findings illustrate that successful ISSMs in nonprofits should effectively employ three effective strategies in protecting their organizations from cyberattacks. Most often, ISSMs in nonprofits should use a comprehensive cybersecurity strategy as their preferred technique in alleviating cybersecurity threats and data breaches. The effective strategic plans entailed (a) instituting a plan on cybersecurity, (b) protecting access to the system using a password, (c) creating awareness on cybersecurity, (d) implementing security procedures, and (e) conducting training. The essence of the strategic plan is providing the foundation to establish secure business operations.

Secondly, successful ISSM in nonprofits should create cybersecurity awareness as a strategy to ensure cybersecurity protection. Almubark et al. (2016) underscored the need for training and education to increase knowledge and understanding among the employees regarding risks and their duty towards protecting infrastructure assets. The effective interventions on cybersecurity awareness should include (a) understanding protection, (b) understanding third-party vendors, and (c) understanding strategic plans. From the data analysis, it was evident that each of the ISSMs that participated in this study corroborated Almubark et al., confirming cybersecurity awareness as a critical component towards effective cybersecurity strategy.

Thirdly, ISSMs who participated in the study reported that nonprofits prefer dependence on third-party vendors as a strategy to ensure cybersecurity protection. From the data analysis conducted, I established that nonprofits have insufficient in-house cybersecurity skills, knowledge, and abilities, creating the need to rely on trusted third-party suppliers. Each of the ISSMs in this study admitted to depending on third-party vendors to offer protection services against cyberattacks to their organizations. The most effective strategic plans for IT professionals is to: (a) employ secure and trusted operators, (b) limit the ISSMs's liabilities, (c) limit exposure to risk, and (d) take advantage of expert technical support.

Applying these concepts to professional practice entails communicating effective nonprofits ISSMs' strategies towards protecting their organizations against cyber threats and cyberattacks. My research outcome implies that the application of successful ISSMs cybersecurity strategies may provide other nonprofits ISSMs an essential guide on assessment and mitigation of cyber threat vulnerabilities. My study's findings align with the GST because successful ISSMs in nonprofits combine the three main strategies to achieve effective, secure, and sustainable operations.

Implications for Social Change

This research's social change implications include the possible impact of effective cybersecurity strategies for nonprofits' ISSMs to alleviate and prevent potential cybersecurity attacks. One of the most significant challenges that nonprofits ISSMs face is the ability to thwart cyberattacks targeted at their organizations. As the findings in this research study, implementation of practical cybersecurity practices illustrates that nonprofits ISSMs with enhanced understanding of cybersecurity methodologies offer sustainable strategies on cybersecurity to alleviate future cyberattacks and boost their prospective for sustainable organizational operations. The sustainability of the nonprofits guarantees society uninterrupted benefits, including driving economic growth through employment opportunities, fostering civic engagement, and promoting leadership capabilities.

As noted in the research study's findings, successful ISSMs in nonprofits should apply several approaches to avert cybersecurity attacks, including (a) cybersecurity strategy, (b) cybersecurity awareness, and (c) dependence on third-party vendor services and infrastructure. Applying these strategies may inspire consumer confidence to the extent of creating greater economic prosperity. Positive social change implications include empowering other ISSMs in nonprofits, academic institutions, and new not-for-profit organizations with practical strategies and resources that benefit the entire community. The benefits to the community include providing employment opportunities, provide an avenue for capturing public attention regarding societal issues, and enabling communities to bypass specific issues affecting them. Furthermore, nonprofits ISSMs may change their perspective about cybersecurity strategies, expand operations, and assist other nonprofits. ISSMs survive cyber breaches and attacks to achieve growth by employing residents within the community and stimulating the general socioeconomic life cycle.

Recommendations for Action

This qualitative multicase study intended to explore the strategies that ISSMs at nonprofit organizations employ in protecting against cyberattacks. In general, up to 3% of nonprofits report cases of stolen or lost data (Romanosky, 2016). In the past, many considered cyberattacks as though it was a problem affecting for-profit organizations only. However, increased cyberattack cases among nonprofit organizations continue affecting their very existence and operations (Carrapico & Farrand, 2017). Presently, however, executives in nonprofits acknowledge cyberattacks' existence and express cybersecurity concerns, but there is a significant gap between the worry and taking of action (Romanosky, 2016).

This research study focused on analyzing numerous scholarly literature sources, nonprofits ISSMs participant interview responses, and archival documents, all of which offered corroborative support as well as triangulation during the process of data collection, to answer the research question of what are the strategies that ISSMs at nonprofit organizations employ to protect against cyberattacks? Based on the triangulated data analysis and the coded node responses’ frequencies, three significant themes came out: (a) cybersecurity strategy, (b) cybersecurity awareness, and (c) dependence on third-party vendor services and infrastructure.

Basing on unique, practical strategies that ISSMs at nonprofits use to avert cyberattacks, I recommend the following actions for executives of nonprofits, future ISSMs at nonprofits, and new nonprofit organizations in general to secure their information using the best cybersecurity interventions:

1. Evaluate cybersecurity health by assessing the current cyber threat environment; classify the organizational data type to protect; identify insider and outsider threats, vulnerabilities, and risks; and emphasizing the types of probable cyber threats.
2. Develop and execute a comprehensive strategic plan on cybersecurity, including policies and procedures targeted at protecting sensitive and likely sensitive data.

The strategic plan on cybersecurity ought to establish the following at a minimum:

a. The two-factor authentication mechanism for valid users (login and password);
b. Company computers with installed antivirus software, malware software, and antispyware; and frequently updated computer operating system patches;
c. Secure Wi-Fi and Internet network connections using data encryption and firewall methodologies.
d. End-to-end encryption of data and tokenization to guarantee secure organizational transactions; and

e. Protecting organization websites using such secure data transaction features as PCI data compliance, firewalls, SSL, and routers.

3. Evaluate in-house IT capacities and consider hiring third-party vendors' services to utilize their expert skills, lower infrastructure liabilities and risks, and alleviate possible data breach losses using the vendor’s data breach warranty on cybersecurity.
4. Create cybersecurity awareness by training the employees to equip them with knowledge on data protection, organizational and consumer data protection, and daily engagement rules to secure successful organizational operations.

My plan on disseminating the study findings and recommendations is to provide summary fact sheets to all the five ISSMs who took part in this study. I will explain to them quite elaborately the research findings and give specific details on how nonprofits can apply the same. I will also share the research outcome and recommendations with academic institutions within the locality, primarily through organized seminars and workshops. Furthermore, as a guest speaker, I will offer consultant services about successful strategies for ISSMs at nonprofits in non-government sponsored workshops and conferences targeting nonprofit organizations. Additionally, I will also seek to exploit industry publications and academic journals to disseminate my research findings.

Recommendations for Further Research

This study’s findings, conclusions, and recommendations may contribute to existing, along with future research about best practices ISSMs at nonprofits employ in protecting and defending their organizations from cyberattacks. The primary outcome of such practices includes achieving successful, sustainable organizational operations. Given that this study covered only nonprofit organizations in Maryland and the District of Columbia, my recommendation is to have other studies conducted in another geographic location. Basing a similar study on a different location and different regional data would enable comparisons with what this research finding has achieved. Moreover, because this study engaged a sample population of five ISSMs, I would recommend that researchers involve a larger sample size in future studies to see whether the results would change or remain similar. Furthermore, my recommendations are that similar studies should engage different populations other than ISSMs and different data collection methods other than interviews in the future. The recommendations will result in a more elaborate finding, which will be more encompassing than the current findings of this study.

In section 1, limitations dealt with whether participants would comprehend the interview questions to the extent of providing honest answers, being available during personal interviews to ensure timely data collection, and whether conducting semistructured interviews and assessing archival company documents would give adequate data answering the overarching research question. The specific limiting factor influencing the research process was finding ISSMs working at nonprofit organizations in Maryland and DC and willing to participate in the study. The finding took time and eventually meant that I take more time seeking to obtain viable research participants. Nonetheless, once the ISSMs agreed to participate, no further significant issues came up. The available archival data and the interviews resulted in honest responses from the participants, thereby providing sufficient data for analyses. In the future, I recommend that researchers should a lot more time to enable the searching of viable research participants.

Reflections

Working towards completing this DIT Doctoral Study has offered me a remarkable growth experience. This process has been fruitful and eventful at the same time because I encountered numerous prolific situations that were beyond my imaginations. I have attained more knowledge regarding effective cybersecurity strategies in nonprofit organizations, which have proven effective in thwarting cybersecurity threats. More specifically, I have learned about the strategic practices that ISSMs at nonprofit organizations in Maryland and DC employ to address cybersecurity challenges. I am optimistic about sharing and applying my research findings with academic institutions, nonprofit organizations, academic institutions, and government entities. The research study's findings may add a lot more content to the existing and future research, especially in equipping ISSMs to protect and safeguard their nonprofit organizations against cyberattacks. Such skilled ISSMs would, in turn, register effective sustainable and secure organizational operations.

After the conduction of literary research, a personal bias formed a preconceived notion that most ISSMs were unaware of and failed to implement sufficient cybersecurity interventions to address potential cyber threat vulnerabilities. Moreover, my experience and expertise in the IT subject area working for different organizations with elaborate cybersecurity plans fueled this idea. All the participants successfully served as ISSMs in nonprofit organizations and understood quite clearly the vulnerabilities of cyber threats, including the potential consequences afflicting their organizational operations. As I conducted the semistructured interviews, I ensured not to lead or direct the participants, including avoiding negative or positive reactions towards their responses. I believe that respondents provided honest and candid answers to all the twelve interview questions. I am also confident that my actions never, at any given time, adversely influence the participants' responses.

Upon completing my research study, the preconceived notion that I had changed about successful ISSMs at nonprofits employs effective cybersecurity strategies. The literature review presented results indicating the use of third-party vendors as risky and costly. However, after analyzing participant interviews and the archival documents data, my thinking changed. Effective ISSMs at nonprofit organizations assessed their risks and generally determined third-party vendors as adaptable and scalable, reliable in their expertise, and cost-effective. Moreover, effective ISSMs established the fact that third-party vendors limited their liabilities whenever data breaches occurred. Although this research study's focus involved only a small population in Maryland and DC, the study's findings most likely capture the general picture of ISSMs at nonprofits in other geographical areas and implement strategic actions against cybersecurity threats.

Conclusion

This qualitative multiple case study intended to explore the strategies that ISSMs at nonprofit organizations employ in protecting against cyberattacks. The research study's findings reveal effective strategies that ISSMs at nonprofit organizations employ towards shielding their organizations from cyberattacks. Three main themes materialized regarding the research findings, corroborating with the literature review, the GST conceptual framework, and the existing body of knowledge. The research study's findings point to the following about ISSMs at nonprofit organizations; (a) implement a cybersecurity strategy geared towards protecting, defending, and reacting to cyberattacks; (b) are mindful of cybersecurity threats, and (c) depend on third-party vendors for services infrastructure and cybersecurity defense. ISSMs at nonprofit organizations who thwart cyberattacks successfully may contribute immensely to economic growth because they employ residents within the community, which eventually stimulates the socioeconomic lifecycle.

Additionally, ISSMs at nonprofit organizations implementing effective strategies may inspire consumer confidence, which would, in turn, trigger significant economic prosperity. In reality, the global cybersecurity threat keeps changing over time, which bestows greater responsibility on the ISSMs to assess the vulnerabilities and develop and execute the best cybersecurity strategies. In turn, it guarantees secure and sustainable operations for nonprofit organizations.

References

Abouelmehdi, K., Beni-Hessane, A., & Khaloufi, H. (2018). Big healthcare data: Preserving security and privacy. *Journal of Big Data, 5*(1), 1-27 https://doi.org/10.1186/s40537-017-0110-7

Abouelmehdi, K., Beni-hssane, A., Khaloufi, H., & Saadi, M. (2017). Big data security and privacy in healthcare: A review. *Procedia Computer Science 113*(2017), 73-80. https://doi.org/10.1016/j.procs.2017.08.292

Adams, M. (2017). Big data and individual privacy in the age of the internet of things. *Technology Innovation Management Review*, 7(4), 12-24. https://doi.org/10.22215/timreview1067

Adashi, E. Y., Walters, L. B., & Menikoff, J. A. (2018). The Belmont Report at 40: Reckoning with time. *American Journal of Public Health*, *108*, 1345–1348. https://doi.org/10.2105/ajph.2018.304580

Adauto, L. S., & Guerrini, F. M. (2018). Self-organized innovation networks from the perspective of complex systems. *Journal of Organizational Change Management, 31*(5), 962-983. https://doi.org/10.1108/JOCM-10-2016-0210

Akaeze, C. O. (2016). Exploring strategies required for small business sustainability in competitive environments (Doctoral dissertation). ProQuest Digital Dissertations & Theses database. (UMI No. 3746398)

Alabady, S. A., Al-Turjman, F., & Din, S. (2018). A novel security model for cooperative virtual networks in the IoT era. *International Journal of Parallel Programming*, *48*(2), 280-295. https://doi.org/10.1007/s10766-018-0580-z

Alhassan, I., Sammon, D., & Daly, M. (2016). Data governance activities: an analysis of the literature. *Journal of Decision Systems*, *25*(sup1), 64–75. https://doi.org/10.1080/12460125.2016.1187397

Alkalbani, A., Deng, H., Kam, B., & Zhang, X. (2017). Information security compliance in organizations: An institutional perspective. *Data and Information Management, 1(2),* 104-114. https://doi.org/10.1515/dim-2017-0006

Almubark, A., Hatanaka, N., Uchida, O., & Ikeda, Y. (2016). Identifying the mechanisms of information security incidents through corporate culture variables and sampling. *International Journal of Cyber-Security and Digital Forensics*, *5*(2), 61-74. https://doi.org/10.17781/p002025

Alshahrani, M., & Traore, I. (2019). Secure mutual authentication and automated access control for IoT smart home using cumulative Keyed-hash chain. *Journal of Information Security and Applications, 45*, 156-175. https://doi.org/10.1016/j.jisa.2019.02.003

Al-Taie, M., Lane, M., & Cater-Steel, A. (2018). An empirical assessment of the CIO role expectations instrument using PLS path modelling. *Communications of the Association for Information Systems, 42*, 1–20. https://doi.org/10.17705/1cais.04201

Anand, R., Medhavi, S., Soni, V., Malhotra, C., & Banwet, D. K. (2018). Transforming information security governance in India (A SAP-LAP based case study of security, IT policy and e-governance). *Information and Computer Security, 26*(1), 58-90. https://doi.org/10.1108/ics-12-2016-0090

Aranda, M., Hurtado, M.D. & Topa, G. (2018). Breach of psychological contract and organizational citizenship behaviors in volunteerism: The mediator role of affect and the moderation of volunteers' age. *Voluntas, 29***,** 59–70. https://doi.org/10.1007/s11266-017-9923-4

Assarroudi, A., Nabavi, F. H., Armat, M. R., Ebadi, A., & Vaismoradi, M. (2018). Directed qualitative content analysis: The description and elaboration of its underpinning methods and data analysis process. *Journal of Research in Nursing*, *23*(1), 1-14. https://doi.org/10.1177/174498711774166

Atoum, I., & Otoom, A. (2016). Holistic performance model for cyber security implementation frameworks. *International Journal of Security and Its Applications, 10*(3), 111-120. https://doi.org/10.14257/ijsia.2016.10.3.10

Attaran, M. (2017). Cloud computing technology: Leveraging the power of the internet to improve business performance. *Journal of International Technology and Information Management, 26*(1), 112-137. https://doi.org/10.1016/j.ijinfomgt.2012.04.001.3

Azungah, T. (2018). Qualitative research: Deductive and inductive approaches to data analysis. *Qualitative Research Journal, 18*(4), 383-400. https://doi.org/10.1108/qrj-d-18-00035

Bach-Mortensen, A. M., & Montgomery, P. (2018). What are the barriers and facilitators for third sector organisations (non-profits) to evaluate their services? A systematic review. *Systematic Reviews*, *7*(1). 1-15. https://doi.org/10.1186/s13643-018-0681-1

Ballaro, J. M., & Polk, L. (2017). Developing an organization for future growth using succession planning. *Organization Development Journal*, *35*(4), 41–42. https://www.isodc.org/page-1730212

Bamkin, M., Maynard, S., & Goulding, A. (2016). Grounded theory and ethnography combined. *Journal of Documentation, 72*(2), 214-231. https://doi.org/10.1108/JD-01-2015-0007

Barlette, Y., Gundolf, K., & Jaouen, A. (2017). CEOs' information security behavior in SMEs: Does ownership matter? *Systèmes d'Information Et Management, 22*(3), 7-45,117. https://doi.org/10.3917/sim.173.0007

Baseri, Y., Hafid, A., & Cherkaoui, S. (2018). Privacy preserving fine-grained location-based access control for mobile cloud. *Computers & Security, 73*, 249-265. https://doi.org/10.1016/j.cose.2017.10.014

Baskerville, R. (2010). Third-degree conflicts: Information warfare. *European Journal of Information Systems, 19*(1,) 1-4. https://doi.org/10.1057/ejis.2010.2

Bauer, S., Bernroider, E. W., & 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*, 145–159. https://doi.org/10.1016/j.cose.2017.04.009

Benoot, C., Hannes, K., & Bilsen, J. (2016). The use of purposeful sampling in a qualitative evidence synthesis: A worked example on sexual adjustment to a cancer trajectory. *BMC Medical Research Methodology, 16*(1)*,* 1-12. https://doi.org/10.1186/s12874-016-0114-6

Bertoglio, D., & Zorzo, A. F. (2017). Overview and open issues on penetration test. *Journal of the Brazilian Computer Society*, *23*(1), 1 https://doi.org/10.1186/s13173-017-0051-1

Bharathi, S. V. (2017). Prioritizing and Ranking the Big Data Information Security Risk Spectrum. *Global Journal of Flexible Systems Management*, *18*(3), 183–201. https://doi.org/10.1007/s40171-017-0157-5

Bidgoli, H. (2018). Cloud computing deployment: What have we learned from real life implementations and practices. *Journal of Strategic Innovation and Sustainability, 13*(1), 36-52. https://doi.org/10.33423/jsis.v13i1.594

Bildosola, I., Río-Belver, R., Cilleruelo, E., & Garechana, G. (2015). Design and implementation of a cloud computing adoption decision tool: Generating a cloud road. *PLOS ONE, 10*(7), e0134563. https://doi.org/10.1371/journal.pone.0134563

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

Boell, S. K., & Cecez-Kecmanovic, D. (2015). Debating systematic literature reviews (SLR) and their ramifications for IS: A rejoinder to Mike Chiasson, Briony Oates, Ulrike Schultze, and Richard Watson. *Journal of Information Technology*, *30*(2), 188-193. https://doi.org/10.1057/jit.2015.15

Bordoff, S., Chen, Q., & Yan, Z. (2017). Cyberattacks, contributing factors, and tackling strategies: The current status of the science of cybersecurity. *Journal International Journal of Cyber Behavior, Psychology and Learning archive, 7*(4), 68-82. https://doi.org/10.4018/ijcbpl.2017100106

Bradshaw, C., Atkinson, S., & Doody, O. (2017). Employing a qualitative description approach in health care research. *Global Qualitative Nursing Research*, *4*, 233339361774228. https://doi.org/10.1177/2333393617742282

Bridgen, S. (2017). Using systems theory to understand the identity of academic advising: A case study. *NACADA Journal, 37*(2), 9-20. https://doi.org/10.12930/NACADA-15-038

Brown, A., & Danaher, P. A. (2017). CHE principles: Facilitating authentic and dialogical semi-structured interviews in educational research. *International Journal of Research & Method in Education*, *42*(1), 76-90. https://doi.org/10.1080/1743727x.2017.1379987

Burns, A. J., Posey, C., Courtney, J. F., Roberts, T. L., & Nanayakkara, P. (2015). Organizational information security as a complex adaptive system: Insights from three agent-based models. *Information Systems Frontiers*, *19*(3), 509-524. https://doi.org/10.1007/s10796-015-9608-8

Cameron, R., Sankaran, S., & Scales, J. (2015). Mixed methods use in project management research. *Project Management Journal*, *46*(2), 90-104. https://doi.org/10.1002/pmj.21484

Carrapico, H., & Farrand, B. (2016). 'Dialogue, partnership and empowerment for network and information security': The changing role of the private sector from objects of regulation to regulation shapers. *Crime, Law and Social Change*, *67*(3), 245-263. https://doi.org/10.1007/s10611-016-9652-4

Cataldi, S. (2018). A proposal for the analysis of the relational dimension in the interview techniques: A pilot study on in-depth interviews and focus groups. *Quality and Quantity, 52*(1), 295-312. https://doi.org/10.1007/s11135-017-0468-9

Catota, F. E., Morgan, M. G., & Sicker, D. C. (2018). Cybersecurity incident response capabilities in the Ecuadorian financial sector. *Journal of Cybersecurity, 4*(1), 1-20. https://doi.org/10.1093/cybsec/tyy002

Cavalcanti, M. F. R. (2017). Guidelines for qualitative research in organization studies: controversy and possibilities. *Administração: Ensino e Pesquisa, 18*(3), 457-488. https://doi.org/10.13058/raep.2017.v18n3.522

Caws, P. (2015). General systems theory: Its past and potential. *Systems Research and Behavioral Science, 32*(5), 514-521. https://doi.org/10.1002/sres.2353

Cerniglia, J. A., Fabozzi, F. J., & Kolm, P. N. (2016). Best practices in research for quantitative equity strategies. *Journal of Portfolio Management, 42*(5), 135-143. https://doi.org/10.3905/jpm.2016.42.5.135

Che-Hung, L., Jen, S. W., & Ching-Wei, L. (2017). The concepts of big data applied in personal knowledge management. *Journal of Knowledge Management, 21*(1), 213-230. https://doi.org/10.1108/JKM-07-2015-0298

Chen, D., Doumeingts, G., & Ducq, Y. (2012). A contribution of system theory to sustainable enterprise interoperability science base. *Computers in Industry*, *63*, 844-857. https://doi.org/10.1016/j.compind.2012.08.005

Citera, E. (2017). Keynes' and the Santa Fe Institute's complexity: same concepts, different methods? *Annals of the Fondazione Luigi Einaudi, 1,* 207-222. https://doi.org/10.26331/1010

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

Cobb, C., Sudar, S., Reiter, N., Anderson, R., Roesner, F., & Kohno, T. (2018). Computer security for data collection technologies. *Development Engineering, 3,* 1-11. https://doi.org/10.1016/j.deveng.2017.12.002

Coetzee, C., Dewald, V. N., & Raju, E. (2016). Disaster resilience and complex adaptive systems theory. *Disaster Prevention and Management, 25*(2), 196-211. https://doi.org/10.1108/dpm-07-2015-0153

Colorafi, K. J., & Evans, B. (2016). Qualitative descriptive methods in health science research. *Health Environments Research & Design Journal, 9*(4), 16-25. https://doi.org/10.1177/1937586715614171

Conrad, L. Y., & Tucker, V. M. (2019). Making it tangible: Hybrid card sorting within qualitative interviews. *Journal of Documentation, 75*(2), 397-416. https://doi.org/10.1108/jd-06-2018-0091

Constantinou, C. S., Georgiou, M., & Perdikogianni, M. (2017). A comparative method for themes saturation (CoMeTS) in qualitative interviews. *Qualitative Research,* 17(5), 571–588. https://doi.org/10.1177/1468794116686650

Corti, L., & Fielding, N. (2016). Opportunities from the digital revolution: Implications for researching, publishing, and consuming qualitative research. *Sage Open, 6*(4), 1-13. https://doi.org/10.1177/2158244016678912

Daher, M., Carré, D., Jaramillo, A., Olivares, H., & Tomicic, A. (2017). Experience and meaning in qualitative research: A conceptual review and a methodological device proposal. *Forum: Qualitative Social Research*, *18*(3), 1-24. https://doi.org/10.17169/fqs-18.3.2696

Daniel Ani, U. P., He, H. M., & Tiwari, A. (2016). Human capability evaluation approach for cyber security in critical industrial infrastructure. In D. Nicholson (Ed.), *Advances in human factors in cybersecurity. Advances in Intelligent systems and computing* (Vol. 501, pp. 169-182). Springer. https://doi.org/10.1007/978-3-319-41932-9_14

Daniel, B. K. (2018). Empirical verification of the "TACT" framework for teaching rigour in qualitative research methodology. *Qualitative Research Journal, 18*(3), 262-275. https://doi.org/10.1108/qrj-d-17-00012

Das, R., Jain, K. K., & Mishra, S. K. (2018). Archival research: A neglected method in organization studies. *Benchmarking, 25*(1), 138-155. https://doi.org/10.1108/bij-08-2016-0123

Dasgupta, M. (2015). Exploring the relevance of case study research. *Vision, 19*(2), 147-160. https://doi.org/10.1177/0972262915575661

Davidson, E., Edwards, R., Jamieson, L., & Weller, S. (2019). Big data, qualitative style: A breadth-and-depth method for working with large amounts of secondary qualitative data. *Quality and Quantity, 53*(1), 363-376. https://doi.org/10.1007/s11135-018-0757-y

De Boer, L., & Andersen, P. H. (2016). Learning from intelligent conversation. *IMP Journal, 10*(3), 512-539. https://doi.org/10.1108/imp-12-2015-0070

DeGama, N., Elias, S., & Peticca-Harris, A. (2019). The good academic: Re-imagining good research in organization and management studies. *Qualitative Research in Organizations and Management: An International Journal*, *14*(1), 2-9. https://doi.org/10.1108/qrom-03-2019-681

DiMase, D., Collier, Z. A., Heffner, K., & Linkov, I. (2015). Systems engineering framework for cyber physical security and resilience. *Environment Systems and Decisions*, *35*(2), 291-300. https://doi.org/10.1007/s10669-015-9540-y

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. https://doi.org/10.1177/1715163517701470

Doll, J. L. (2017). Structured interviews: Developing interviewing skills in human resource management courses. *Management Teaching Review, 3*(1), 46-61. https://doi.org/10.1177/2379298117722520

Dove, E. S. (2018). The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era. *The Journal of Law, Medicine & Ethics, 46*(4), 1013–1030. https://doi.org/10.1177/1073110518822003

Drack, M., & Pouvreau, D. (2015). On the history of Ludwig von Bertalanffy's "General Systemology", and on its relationship to cybernetics - part III: convergences and divergences. *International journal of general systems*, *44*(5), 523–571. https://doi.org/10.1080/03081079.2014.1000642

Efthymiopoulos, M. P. (2019). A cyber-security framework for development, defense and innovation at NATO. *Journal of Innovation and Entrepreneurship, 8*(1). 1-26. https://doi.org/10.1186/s13731-019-0105-z

El-Bendary, M. (2017). FEC merged with double security approach based on encrypted image steganography for different purpose in the presence of noise and different attacks. *Multimedia Tools and Applications, 76*(24), 26463-26501. https://doi.org/10.1007/s11042-016-4177-5

Elman, C., Gerring, J., & Mahoney, J. (2016). Case study research. *Sociological Methods & Research, 45,* 375-391. https://doi.org/10.1177/0049124116644273

Eriksson, P. E. (2017). Procurement strategies for enhancing exploration and exploitation in construction projects. *Journal of Financial Management of Property and Construction, 22*(2), 211-230. https://doi.org/10.1108/jfmpc-05-2016-0018

Erlingsson, C., & Brysiewicz, P. (2017). A hands-on guide to doing content analysis. *African Journal of Emergency Medicine, 7*(3), 93-99. https://doi.org/10.1016/j.afjem.2017.08.001

Fal', O. M. (2017). Standardization in information technology security. *Cybernetics and Systems Analysis, 53*(1), 78-82. https://doi.org/10.1007/s10559-017-9908-8

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

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision Support Systems, 86*, 13-23. https://doi.org/10.1016/j.dss.2016.02.012

Fletcher, A. J. (2017). Applying critical realism in qualitative research: Methodology meets method. *International Journal of Social Research Methodology: Theory & Practice, 20,* 181-194. https://doi.org/10.1080/13645579.2016.1144401

Fusch, P., Fusch, G. E., & Ness, L. R. (2018). Denzin's Paradigm Shift: Revisiting Triangulation in Qualitative Research. *Journal of Social Change*, *10*(1), 19–32. https://doi.org/10.5590/JOSC.2018.10.1.02

Gammelgaard, B. (2017). Editorial: The qualitative case study. *International Journal of Logistics Management, 28*(4), 910-913. https://doi.org/10.1108/IJLM-09-2017-0231

Garlinec, D., Možnik, D., & Guberina, B. (2017). Cybersecurity and cyber defence: National level strategic approach. *Journal for Control, Measurement, Electronics, Computing and Communications, 58*(3), 273-286. https://doi.org/10.1080/00051144.2017.1407022

Gaus, N. (2017). Selecting research approaches and research designs: A reflective essay. *Qualitative Research Journal, 17*(2), 99-112. https://doi.org/10.1108/QRJ-07-2016-0041

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). Increasing cybersecurity investments in private sector firms. *Journal of Cybersecurity, 1*(1), 3-17 https://doi.org/10.1093/cybsec/tyv011

Greenwood, M. (2016). Approving or improving research ethics in management journals. *Journal of Business Ethics, 137*(3), 507-520. https://doi.org/10.1007/s10551-015-2564-x

Grimaldo, F., Marušić, A., & Squazzoni, F. (2018). Fragments of peer review: A quantitative analysis of the literature (1969-2015). *PLoSONE, 13*(2), e0193148. https://doi.org/10.1371/journal.pone.0193148

Hammarberg, K., Kirkman, M., & de Lacey, S. (2016). Qualitative research methods: when to use them and how to judge them. *Human Reproduction, 31*(3), 498–501. https://doi.org/10.1093/humrep/dev334

Hampton, J. O., MacKenzie, D. I., & Forsyth, D. M. (2019). How many to sample? Statistical guidelines for monitoring animal welfare outcomes. *PLOS ONE*, *14*(1), e0211417. https://doi.org/10.1371/journal.pone.0211417

He, W., & Zhang, Z. (2019). Enterprise cybersecurity training and awareness programs: Recommendations for success. *Journal of Organizational Computing and Electronic Commerce, 29*(4), 249-257. https://doi.org/10.1080/10919392.2019.1611528

Heesen, R., Bright, L. K., & Zucker, A. (2016). Vindicating methodological triangulation. *Synthese, 196*(8), 3067-3081. https://doi.org/10.1007/s11229-016-1294-7

Hennink, M. M., Kaiser, B. N., & Marconi, V. C. (2017). Code saturation versus meaning saturation: How many interviews are enough? *Qualitative Health Research, 27,* 591-608. https://doi.org/10.1177/1049732316665344

Henry, C., & Foss, L. (2015). Case sensitive? A review of the literature on the use of case method in entrepreneurship research. *International Journal of Entrepreneurial Behaviour & Research, 21*(3), 389-409. https://doi.org/10.1108/IJEBR-03-2014-0054

Hodiamont, F., Jünger, S., Leidl, R., Bernd, O. M., Schildmann, E., & Bausewein, C. (2019). Understanding complexity – the palliative care situation as a complex adaptive system. *BMC Health Services Research, 19.* https://doi.org/10.1186/s12913-019-3961-0

Hof, B. E. (2018). The cybernetic "general model theory": Unifying science or epistemic change? *Perspectives on Science, 26*(1), 76. http://search.ebscohost.com/login.aspx?direct=true&db=edb&AN=127769651&site=eds-live

Holland, A. (2017). Nonprofit leaders' strategies in capturing the attention of committed, large donors (Doctoral dissertation). ProQuest Digital Dissertations & Theses Global database. (UMI No. 10253906)

Holtfreter, R. E., & Harrington, A. (2015). Data breach trends in the united states. *Journal of Financial Crime, 22*(2), 242-260. https://doi.org/10.1108/JFC-09-2013-0055

Horne, C. A., Ahmad, A., & Maynard, B. S. (2016, December). *A theory on information security* [Paper presentation]. The 27th Australasian Conference on Information Systems, Wollongong, Australia.

https://www.researchgate.net/publication/318589055_A_Theory_on_Information_Security

Horvath, M., & Lovasz, A. (2018). Programming the vicious circle: Austen, Deleuze and viral repetition. *Rhizomes: Cultural Studies in Emerging Knowledge,* (33), 15. http://www.rhizomes.net/issue33/pdf/horvath.pdf

Hubbard, T., Fabius, J. A., & Steinhoff, J. C. (2019). Harnessing and protecting data assets in a 21st century financial enterprise. *Journal of Government Financial Management, 67*(4), 34-41. https://institutes.kpmg.us/content/dam/institutes/en/government/pdfs/2019/aga-winter-cyber.pdf

Humphreys, M. (2015). Reflections on the ethics of social experimentation. *Journal of Globalization and Development, 6*(1), 87-112. https://doi.org/10.1515/jgd-2014-0016

International Federation of Red Cross and Red Crescent Societies. (2019). Volunteering policy. Retrieved February 26, 2019, from https://media.ifrc.org/ifrc/what-we-do/volunteers/volunteering-policy/

Iivari, N. (2018). Using member checking in interpretive research practice. *Information Technology & People, 31*(1), 111-133. https://doi.org/10.1108/ITP-07-2016-0168

Jagalur, P. K., Levin, P. L., Brittain, K., Dubinsky, M., Landau-Jagalur, K., & Lathrop, C. (2018, November). *Cybersecurity for civil society*. In 2018 IEEE International Symposium on Technology and Society (ISTAS; pp. 102-107). IEEE.

Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in Hospitals: A Systematic, Organizational Perspective. *Journal of Medical Internet Research, 20*(5), 1-16. https://doi.org/10.2196/10059

Junior, N. D. S. F. D. (2016). Dynamic quality cost model based on complexity theory. *International Journal of Quality & Reliability Management, 33*(5), 633-653. https://doi.org/10.1108/ijqrm-07-2014-0085

Kajiyama, T., Jennex, M., & Addo, T. (2017). To cloud or not to cloud: How risks and threats are affecting cloud adoption decisions. *Information and Computer Security, 25*(5), 634-659. https://doi.org/doi.org/10.1108/ICS-07-2016-0051

Kallio, H., Pietilä, A., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: Developing a framework for a qualitative semistructured interview guide. *Journal of Advanced Nursing, 72,* 2954-2965. https://doi.org/10.1111/jan.13031

Kayaalp, M. (2018). Patient privacy in the era of big data. *Balkan Medical Journal, 35*(1), 8–17. https://doi.org/10.4274/balkanmedj.2017.0966

Kholidy, H. A., Erradi, A., Abdelwahed, S., & Baiardi, F. (2016). A risk mitigation approach for autonomous cloud intrusion response system. *Computing*, *98*(11), 1111–1135. https://doi.org/10.1007/s00607-016-0495-8

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

Kordova, S. K., Frank, M., & Miller, A. S. (2018). Systems thinking education—Seeing the forest through the trees. *Systems,* 6(3), 29. https://doi.org/10.3390/systems6030029

Korrapati, R. (2016). *Five chapter model for research thesis writing: 108 practicallLessons.* Diamond Pocket Books.

Krippner, S., Ruttenber, A. J., Engelman, S. R., & Granger, D. L. (1985). Toward the application of general systems theory in humanistic psychology. *Systems Research, 2*(2), 105–115. https://doi.org/10.1002/sres.3850020203

Kristof, V. A., Verschraegen, G., Valentinov, V., & Gruezmacher, M. (2019). The social, the ecological, and the adaptive. Von Bertalanffy's general systems theory and the adaptive governance of social□ecological systems. *Systems Research and Behavioral Science, 36*(3), 308-321. https://doi.org/10.1002/sres.2587

Kude, T., Hoehle, H., & Sykes, T. A. (2017). Big data breaches and customer compensation strategies. *International Journal of Operations & Production Management*, *37*(1), 56-74. https://doi.org/10.1108/IJOPM-03-2015-0156

Kuerbis, B., & Badiei, F. (2017). Mapping the cybersecurity institutional landscape", *Digital Policy, Regulation and Governance*, *19*(6), 466-492. https://doi.org/10.1108/DPRG-05-2017-0024

Lanz, J. (2017). The Chief Information Security Officer: The New CFO of Information Security. *CPA Journal, 87*(6), 52. https://www.cpajournal.com/2017/06/23/chief-information-security-officer/

Larkin, M., Shaw, R., & Flowers, P. (2019). Multiperspectival designs and processes in interpretative phenomenological analysis research. *Qualitative Research in Psychology, 16*(2), 182-198. https://doi.org/10.1080/14780887.2018.1540655

Lee, C. I. S. G. (2016, March 11). Big Data in Management Research (No. EPS-2016-365-ORG). ERIM Ph.D. Series Research in Management. Erasmus University Rotterdam. http://hdl.handle.net/1765/79818

Leung, L. (2015). Validity, reliability, and generalizability in qualitative research. *Journal of family medicine and primary care*, *4*(3), 324. https://doi.org/10.4103/2249-4863.161306

Levesque, R., Walsh, D., & Whyte, D. (2015). Securing cyberspace: Towards an agenda for research and practice. *Technology Innovation Management Review, 5*(11), 26-34. https://search.proquest.com/docview/1736797748?accountid=45049

Libicki, M. (2017a). The convergence of information warfare. *Strategic Studies Quarterly, 11*(1), 49-65. http://www.jstor.org/stable/26271590

Libicki, M. C. (2017b). Second acts in cyberspace. *Journal of Cybersecurity, 3*(1), 29–35. https://doi.org/10.1093/cybsec/tyw014

Lim, C., Kim, M., Kim, K., Kim, K., & Maglio, P. P. (2018). Using data to advance service: Managerial issues and theoretical implications from action research. *Journal of Service Theory and Practice, 28*(1), 99-128. https://doi.org/10.1108/JSTP-08-2016-0141

Liu, Y.-T., Du, D., Xia, Y.-B., Chen, H.-B., Zang, B.-Y & Liang, Z. (2018). SplitPass: A mutually distrusting two-party password manager. *Journal of Computer Science and Technology, 33*(1), 98-115. https://doi.org/10.1007/s11390-018-1810-y

Lucas, S. R. (2016). Where the rubber meets the road: Probability and nonprobability moments in experiment, interview, archival, administrative, and ethnographic data collection. *Socius, 2,* 2378023116634709.

MacDougall, R. (2019). Sympathetic physics: The keely motor and the laws of thermodynamics in nineteenth-century culture. *Technology and Culture, 60*(2), 438-466. https://doi.org/10.1353/tech.2019.0031

Madill, A., & Sullivan, P. (2018). Mirrors, portraits, and member checking: Managing difficult moments of knowledge exchange in the social sciences. *Qualitative Psychology*, *5*(3), 321–339. https://doi.org/10.1037/qup0000089

Majid, M. A., Othman, M., Mohamad, S. F., Lim, S. A., & Yusof, A. (2017). Piloting for interviews in qualitative research: Operationalization and lessons learnt. *International Journal of Academic Research in Business and Social Sciences, 7*(4). https://doi.org/10.6007/ijarbss/v7-i4/2916

Malgieri, G., & Comandé, G. (2017). Why a right to legibility of automated decision-making exists in the general data protection regulation. *International Data Privacy Law, 7*(4), 243-265. https://doi.org/10.1093/idpl/ipx019

Maras, M.-H. (2015). Internet of Things: Security and Privacy Implications. *International Data Privacy Law, 5*(2), 99–104. https://doi.org/10.1093/idpl/ipv004

Marchisotti, G. G., Joia, L. A., & De Carvalho, R. B. (2019). The social representation of cloud computing according to Brazilian information technology professionals. *Revista De Administração De Empresas, 59*(1), 16-28. https://doi.org/10.1590/S0034-759020190103

Margaret, M. M. (2016). Case study research: What, why and how? *South Asian Journal of Management, 23*(3), 218-221. https://search.proquest.com/docview/1845776117?accountid=45049

Marshall, C., & Rossman, G. B. (2016). Designing qualitative research (6th ed.). Sage.

Martin, K., & Murphy, P. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, *45*(2), 135–155. https://doi.org/10.1007/s11747-016-0495-4

Mason, J. (2018). *Qualitative Researching.* SAGE Publications.

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

Mcintosh, M. J., & Morse, J. M. (2015). Situating and constructing diversity in semi-structured interviews. *Global Qualitative Nursing Research*, *2*, 233339361559767. https://doi.org/10.1177/2333393615597674

McMahon, D., Seaman, S. & Lemley, D. A. (2015). The adoption of websites by nonprofits and the impact on society. *Technology in Society, 42,* 1-8. https://doi.org/10.1016/j.techsoc.2015.01.001

McTate, E. A., & Leffler, J. M. (2017). Diagnosing disruptive mood dysregulation disorder: Integrating semistructured and unstructured interviews. *Clinical Child Psychology & Psychiatry, 22,* 187-203. https://doi.org/10.1177/1359104516658190

Meisner, M. (2018). Financial consequences of cyberattacks leading to data breaches in healthcare sector. *Copernican Journal of Finance & Accounting*, *6*(3), 63. https://doi.org/10.12775/cjfa.2017.017

Mierzwa, S., & Scott, J. (2017). *Cybersecurity in nonprofit and non-governmental organizations.* Institute for Critical Infrastructure Technology. https://www.researchgate.net/publication/314096686_Cybersecurity_in_Non-Profit_and_Non-Governmental_Organizations

Mingers, J., & Standing, C. (2018). What is information? toward a theory of information as objective and veridical. *Journal of Information Technology*, *33(2),* 85-104. https://doi.org/10.1057/s41265-017-0038-6

Mittal, S., Durak, U., & Ören, T. I. (2017). *Guide to simulation-based disciplines: Advancing our computational future*. Springer.

Mohajan, H. K. (2018). Qualitative research methodology in social sciences and related subjects. *Journal of Economic Development, Environment and People, 7*(1), 23-48. https://doi.org/10.26458/jedep.v7i1.571

Mohammed, S., Ramkumar, L., & Rajasekar, V. R. (2017). Password-based Authentication in Computer Security: Why is it still there? *The SIJ Transactions on Computer Science Engineering & its Applications (CSEA), 5*(2), 33-36.

https://www.researchgate.net/publication/316350564_Password-based_Authentication_in_Computer_Security_Why_is_it_still_there

Monov, L. B., & Karev, M. L. (2018). Information warfare conceptual framework. International *Journal of Recent Scientific Research, 9*(5F), 26859-26866. https://doi.org/10.24327/IJRSR

Moore, B., Calvo-Amodio, J., & Junker, J. (2017). Applying a framework for complementarist intervention approaches to service organizations to achieve a sustainable holistic management model. *Systemic Practice & Action Research, 30*(5), 487–513. https://doi.org/10.1007/s11213-016-9403-6

Morgan, S. J., Pullon, S. R., Macdonald, L. M., McKinlay, E. M., & Gray, B. V. (2017). Case study observational research: A framework for conducting case study research where observation data are the focus. *Qualitative Health Research, 27(7),* 1060-1068. https://doi.org/10.1177/1049732316649160

Morris, N. S., & Rosenbloom, D. A. (2017). Defining and understanding pilot and other feasibility studies. *American Journal of Nursing, 117*, 38-47. https://doi.org/10.1097/01.NAJ.0000513261.75366.37

Moskal, S., Yang, S. J., & Kuhl, M. E. (2018). Cyber threat assessment via attack scenario simulation using an integrated adversary and network modeling approach. *Journal of Defense Modeling and Simulation, 15*(1), 13–29. https://doi.org/10.1177/1548512917725408

Mowlana, H. (2019). Human communication theory: A five-dimensional model. *Journal of International Communication, 25*(1), 3-33. https://doi.org/10.1080/13216597.2018.1560351

Muegge, S., & Craigen, D. (2015). A design science approach to constructing critical infrastructure and communicating cybersecurity risks. *Technology Innovation Management Review, 5*(6), 6-16. https://search.proquest.com/docview/1697867587?accountid=45049

Muhammad, B. F. (2018). A review of Gadamerian and Ricoeurian hermeneutics and its application to interpretive accounting research. *Qualitative Research in Organizations and Management, 13*(3), 261-283. https://doi.org/10.1108/QROM-07-2017-1550

National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. (1979). The Belmont report: Ethical principles and guidelines for the protection of human subjects of research. Washington, DC: U.S. Department of Health and Human Services.

National Council of Nonprofits. (2016). Economic Impact. https://www.councilofnonprofits.org/economic-impact

Newton, V. L. (2017). 'Its good to be able to talk': An exploration of the complexities of participant and researcher relationships when conducting sensitive research. *Womens Studies International Forum*, *61*, 93–99. https://doi.org/10.1016/j.wsif.2016.11.011

Ngongo, C. J., Frick, K. D., Hightower, A. W., Mathingau, F. A., Burke, H., & Breiman, R. F. (2015). The perils of straying from protocol: Sampling bias and interviewer effects. *PLoS ONE*, *10*(2), 1–11. https://doi.org/10.1371/journal.pone.0118025

Nieuwenhuis, L. J. M., Ehrenhard, M. L., & Prause, L. (2018). The shift to cloud computing: The impact of disruptive technology on the enterprise software business ecosystem. *Technological Forecasting and Social Change, 129*, 308. https://search.proquest.com/docview/2084459733?accountid=45049

Nikolić, D. (2015). Practopoiesis: Or how life fosters a mind. *Journal of Theoretical Biology*, *373*, 40–61. https://doi.org/10.1016/j.jtbi.2015.03.003

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

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,* 1-13. https://doi.org/10.1177/1609406917733847

Oakley, J. G. (2019). The state of modern offensive security. *Professional Red Teaming,* 29-41. https://doi.org/10.1007/978-1-4842-4309-1_3

Ogliastri, E., Jäger, U. P., & Prado, A. M. (2016). Strategy and structure in high-performing nonprofits: Insights from Iberoamerican cases. *Voluntas*, *27*(1), 222-248. https://doi.org/10.1007/s11266-015-9560-8

Pandey, S., & Chawla, D. (2016). Using qualitative research for establishing content validity of e-lifestyle and website quality constructs. *Qualitative Market Research, 19*(3), 339-356. https://doi.org/10.1108/QMR-05-2015-0033

Pardini, D. J., Heinisch, A. M., & Parreiras, F. S. (2017). Cyber Security Governance and Management for Smart Grids in Brazilian Energy Utilities. *Journal of Information Systems and Technology Management, 14*(3), 385-400. https://doi.org/10.4301/s1807-17752017000300006

Park, W., Na, O., & Chang, H. (2016). An exploratory research on advanced smart media security design for sustainable intelligence information system. *Multimedia Tools and Applications, 75*(11), 6059-6070. https://doi.org/10.1007/s11042-014-2393-4

Parks, R., Xu, H., Chu, C. H., & Lowry, P. B. (2017). Examining the intended and unintended consequences of organisational privacy safeguards. *European Journal of Information Systems*, *26*(1), 37-65. https://doi.org/10.1057/s41303-016-0001-6

Pascalev, M. (2017). Privacy exchanges: Restoring consent in privacy self-management. *Ethics and Information Technology, 19*(1), 39-48.

Pearce, G. (2017). Governance, risk, compliance and a big data case study. *ISACA Journal, 6,* 1-7.

Pelosi, L. (2015). The participant as evolving protagonist. *Qualitative Research Journal, 15*(2), 112-120. https://doi.org/10.1108/qrj-01-2015-0003

Pillay, K. (2017). Guest editor’s introduction: AJIC focus section on cybersecurity. *African Journal of Information and Communication, 20,* 79–82. https://doi.org/10.23962/10539/23575

Posey, C., Raja, U., Crossler, R. E., & Burns, A. J. (2017). Taking stock of organisations’ protection of privacy: Categorising and assessing threats to personally identifiable information in the USA. *European Journal of Information Systems, 26*(6), 585-604. https://doi.org/10.1057/s41303-017-0065-y

Pouloudi, N., Currie, W., & Whitley, E. A. (2016). Entangled stakeholder roles and perceptions in health information systems: A longitudinal study of the U.K. NHS N3 network. *Journal of the Association for Information Systems, 17*(2), 107-161. https://doi.org/10.17705/1jais.00421

Prakash, M., & Singaravel, G. (2015). An approach for prevention of privacy breach and information leakage in sensitive data mining. *Computers & Electrical Engineering, 45,* 134-140. https://doi.org/10.1016/j.compeleceng.2015.01.016

Preiser, R., Biggs, R., De Vos, A., & Folke, C. (2018). Social-ecological systems as complex adaptive systems: organizing principles for advancing research methods and approaches. *Ecology and Society*, (4), 46. https://doi.org/10.5751/ES-10558-230446

Proctor, R. W., & Xiong, A. (2018). Adoption of population-level statistical methods did transform psychological science but for the better: Commentary on Lamiell. *American Journal of Psychology*, *131*(4), 483-487. https://doi.org/10.5406/amerjpsyc.131.4.0483

Qu, S. Q., & Dumay, J. (2011). The qualitative research interview. *Qualitative Research in Accounting and Management, 8*(3), 238-264. https://doi.org/10.1108/11766091111162070

Quinney, L., Dwyer, T., & Chapman, Y. (2016). Who, where, and how of interviewing peers. *SAGE Open, 6*(3), 215824401665968. https://doi.org/10.1177/2158244016659688

Quirós, P., Alonso, P., Díaz, I., & Montes, S. (2015). Protecting data: a fuzzy approach. *International Journal of Computer Mathematics, 92*(9), 1989-2000. https://doi.org/10.1080/00207160.2014.928700

Rainie, S., Schultz, J., Briggs, E., Riggs, P., & Palmanteer-Holder, N. L. (2017). Data as a strategic resource: self-determination, governance, and the data challenge for indigenous nations in the United States. *International Indigenous Policy Journal, 8,* https://doi,org/10.18584/iipj.2017.8.2.1

Rajendran, K., Jayabalan, M., & Rana, M. E. (2017). A study on k-anonymity, l-diversity, and t-closeness techniques focusing medical data. I*nternational Journal of Computer Science and Network Security, 17*(12), 172-177. https://www.researchgate.net/publication/322330948_A_Study_on_k-anonymity_l-diversity_and_t-closeness_Techniques_focusing_Medical_Data

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

Rathi, D., & Given, L. M. (2017). Nonprofit organizations' use of tools and technologies for knowledge management: A comparative study. *Journal of Knowledge Management, 21*(4), 718-740. https://doi.org/10.1108/JKM-06-2016-0229

Reddy, A. G., Das, A. K., Odelu, V., & Yoo, K.-Y. (2016). An Enhanced Biometric Based Authentication with Key-Agreement Protocol for Multi-Server Architecture Based on Elliptic Curve Cryptography. *PLoS ONE*, *11*(5), 1–28. https://doi.org/10.1371/journal.pone.0154308

Ridder, H. (2017). The theory contribution of case study research designs. *Business Research*, *10*(2), 281-305. https://doi.org/10.1007/s40685-017-0045-z

Roberts, K., Dowell, A., & Nie, J. (2019). Attempting rigour and replicability in thematic analysis of qualitative research data; a case study of codebook development. *BMC Medical Research Methodology*, *19*(1). doi:10.1186/s12874-019-0707-y

Robins, C. S., & Eisen, K. (2017). Strategies for the effective use of NVivo in a largescale study: Qualitative analysis and the repeal of don't ask, don't tell. *Qualitative Inquiry*, *23*(10), 768-778. https://doi.org/10.1177/1077800417731089

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *Journal of Psychology, 91*(1), 93-114. https://doi.org/10.1080/00223980.1975.9915803

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity, 2*(2), 121–135. https://doi.org/10.1093/cybsec/tyw001

Rossouw, v. S., & Willett, M. (2017). Cloud computing assurance – A review of literature guidance. *Information and Computer Security, 25*(1), 26-46. https://doi.org/10.1108/ICS-09-2015-0037

Rousseau, D. (2015). General systems theory: Its present and potential. *Systems Research and Behavioral Science, 32*(5), 522-533. https://doi.org/10.1002/sres.2354

Rousseau, D., Wilby, J., Billingham, J., & Blachfellner, S. (2018). *General Systemology: Transdisciplinarity for discovery, insight and innovation*. Springer.

Samani, A., Ghenniwa, H. H., & Wahaishi, A. (2015) (2015). Privacy in internet of things: A model and protection framework. *Procedia Computer Science, 52,* 606-613. https://doi.org/10.1016/j.procs.2015.05.046

Sarabi, A., Naghizadeh, P., Liu, Y., & Liu, M. (2016). Risky business: Fine-grained data breach prediction using business profiles. *Journal of Cybersecurity, 2*(1), 15–28. https://doi.org/10.1093/cybsec/tyw004

Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., Burroughs, H. C., Jinks, C. (2018). Saturation in qualitative research: Exploring its conceptualization and operationalization. *Quality and Quantity, 52*(4), 1893-1907. https://doi.org/10.1007/s11135-017-0574-8

Schneider, A., Wickert, C., & Marti, E. (2016). Reducing complexity by creating complexity: A systems theory perspective on how organizations respond to their environments. *Journal of Management Studies*, *54*(2), 182-208. https://doi.org/10.1111/joms.12206

Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems, 32*(2) 314–341. https://doi.org/10.1080/07421222.2015.1063315

Shapiro, Y. (2015). Dynamical Systems Therapy (DST): Theory and practical applications. *Psychoanalytic Dialogues*, *25*(1), 83–107. https://doi.org/10.1080/10481885.2015.991245

Shukla, T. (2016). An introduction to qualitative research. *South Asian Journal of Management, 23*(4), 200-202. https://search.proquest.com/docview/1876464111?accountid=45049

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. https://doi.org/10.1177/1609406915624574

Sommestad, T., Karlzén, 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. https://doi.org/10.1108/ICS-04-2014-0025

Stacey, A. (2016). Militating against data fabrication and falsification: A protocol of trias politica for business research. *Electronic Journal of Business Research Methods, 14*(2), 72-82. https://academic-publishing.org/index.php/ejbrm/article/view/1343/1306

Stewart, H., & Jürjens, J. (2017). Information security management and the human aspect in organizations. *Information and Computer Security*, *25*(5), 494-534. https://doi.org/10.1108/ICS-07-2016-0054

Tahir, R. (2018). A study on malware and malware detection techniques. *International Journal of Education and Management Engineering, 8*(2), 20. https://doi.org/10.5815/ijeme.2018.02.03

Teixeira, B., Gregory, P. A., & Austin, Z. (2017). How are pharmacists in Ontario adapting to practice change? Results of a qualitative analysis using Kotter's change management model. *Canadian Pharmacists Journal / Revue des Pharmaciens du Canada*, *150*(3), 198-205. https://doi.org/10.1177/1715163517701470

Theofanidis, D., & Fountouki, A. (2019). Limitations and delimitations in the research process. *Perioperative Nursing, 7*(3), 155–162. https://doi.org/10.5281/zenodo.2552022

Theophanidis, P., Thibault, G., & Trudel, D. (2017). At the margins of cybernetics. *Canadian Journal of Communication, 42*(3), 397-405. https://doi.org/10.22230/cjc.2017v42n3e3304

Thistoll, T., Hooper, V., & Pauleen, D. J. (2016). Acquiring and developing theoretical sensitivity through undertaking a grounded preliminary literature review. *Quality and Quantity*, *50*(2), 619-636. https://doi.org/10.1007/s11135-015-0167-3

Törmänen, J., Hämäläinen, R. P., & Saarinen, E. (2016). Systems intelligence inventory. *Learning Organization, 23*(4), 218-231. https://doi.org/10.1108/TLO-01-2016-0006

Tumbas, S., Berente, N., & vom Brocke, J. (2018). Digital innovation and institutional entrepreneurship: Chief digital officer perspectives of their emerging role. *Journal of Information Technology (Palgrave Macmillan)*, 33(3), 188–202. https://doi.org/10.1057/s41265-018-0055-0

Turner, J. R., & Baker, R. M. (2019). Complexity theory: An overview with potential applications for the social sciences. *Systems, 7*(1), 4. https://doi.org/10.3390/systems7010004

Van de Pas, J., & van Bussel, G. (2015). 'Privacy Lost - and Found?' The Information Value Chain as a Model to Meet Citizens' Concerns. *The Electronic Journal Information Systems Evaluation, 18*(2), 185-195.

Van den Berg, A., & Struwig, M. (2017). Guidelines for Researchers Using an Adapted Consensual Qualitative Research Approach in Management Research. *Electronic Journal of Business Research Methods*, 15(2). https://search. proquest-com.ezp.waldenulibrary.org/abicomplete/docview/1954333307/BB8F784768FE42F7PQ/1?accountid=14872

Van Rooy, G., Mufune, P., & Amadhila, E. (2015). Experiences and perceptions of barriers to health services for elderly in rural Namibia: A qualitative study. *SAGE Open, 5*(3), 1-10. https://doi.org/10.1177/2158244015596049

Venkatesh, V., Brown, S. A., & Sullivan, Y. W. (2016). Guidelines for conducting mixed-methods research: An extension and illustration. *Journal of the Association for Information Systems, 17*(7), 435-494. https://search.proquest.com/docview/1813158448?accountid=45049

Verhoeff, R. P., Knippels, M. P. J., Gilissen, M. G. R., & Boersma, K. T. (2018). The theoretical nature of systems thinking. Perspectives on systems thinking in biology education. *Frontiers in Education*. https://doi.org/10.3389/feduc.2018.00040

versus practice in published studies using ATLAS and NVivo, 1994-2013. *Social*

von Bertalanffy, L. (1968). General systems theory as integrating factor in contemporary science. *Akten Des XIV. Internationalen Kongresses Für Philosophie*, *2,* 335–340. https://doi.org/10.5840/wcp1419682120

von Bertalanffy, L. (1972). The History and Status of General Systems Theory. *Academy Of Management Journal*, *15*(4), 407-426. https://doi.org/10.2307/255139

Wallace, M., & Sheldon, N. (2015). Business research ethics: Participant observer perspectives: JBE JBE. *Journal of Business Ethics, 128*(2), 267-277. https://doi.org/10.1007/s10551-014-2102-2

Wardale, D., Cameron, R., & Li, J. (2015). Considerations for multidisciplinary, culturally sensitive, mixed methods research. *Electronic Journal of Business Research Methods, 13*(1), 37-47. https://www.semanticscholar.org/paper/Considerations-for-multidisciplinary%2C-culturally-Wardale-Cameron/a42467f63a41ac1d780769d2e5bb0e635e70df47

Wels, H. (2015). "Animals like us": Revisiting organizational ethnography and research. *Journal of Organizational Ethnography, 4*(3), 242-259. https://doi.org/10.1108/JOE-12-2014-0039

Werder, K., & Maedche, A. (2018). Explaining the emergence of team agility: a complex adaptive systems perspective. *Information Technology & People*, *31*(3), 819. http://search.ebscohost.com/login.aspx?direct=true&db=edb&AN=129756201&site=eds-live

Williams, P. A., & Woodward, A. J. (2015). Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. *Medical devices (Auckland, N.Z.), 8,* 305-16.

Williams, T. L., & Needham, C. R. (2016). Transformation of a city: Gentrification's influence on the small business owners of Harlem, New York. *Sage Open, 6*(4), 2158244016673631. https://doi.org/10.1177/2158244016673631

Wolgemuth, J. R., Hicks, T., & Agosto, V. (2017). Unpacking assumptions in research synthesis: A critical construct synthesis approach. *Educational Researcher*, *46*(3), 131–139. https://doi.org/10.3102/0013189X17703946

Wong, T. S., Gaston, A., DeJesus, S., & Prapavessis, H. (2016). The utility of a protection motivation theory framework for understanding sedentary behavior. *Health Psychology and Behavioral Medicine, 4*(1), 29–48. https://doi.org/10.1080/21642850.2015.1128333

Woods, M., Paulus, T., Atkins, D. P., & Macklin, R. (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.

Woszczynski, A. B., & Green, A. (2017). Learning outcomes for cyber defense competitions. *Journal of Information Systems Education, 28*(1), 21-41.

Wright, R. T., Roberts, N., & Wilson, D. (2017). The role of context in IT assimilation: A multi-method study of a SaaS platform in the US nonprofit sector. *European Journal of Information Systems, 26*(5), 509-539. https://doi.org/10.1057/s41303-017-0053-2

Wu, Y. P., Thompson, D., Aroian, K. J., Mcquaid, E. L., & Deatrick, J. A. (2016). Commentary: Writing and Evaluating Qualitative Research Reports. *Journal of Pediatric Psychology, 41*(5), 493-505. https://doi.org/10.1093/jpepsy/jsw032

Xu, X., Wang, B., & Zhou, Y. (2016). A method based on trust model for large group decision-making with incomplete preference information. *Journal of Intelligent & Fuzzy Systems, 30*(6), 3551–3565. https://doi.org/10.3233/ifs-162100

Yang, Y., Pankow, J., Swan, H., Willett, J., Shannon, G. M., Rudes, D. S., & Knight, K. (2018). Preparing for analysis: A practical guide for a critical step for procedural rigor in large-scale multisite qualitative research studies. *Quality and Quantity, 52*(2), 815-828. https://doi.org/10.1007/s11135-017-0490-y

Yang, L., Li, J., Elisa, N., Prickett, T., & Chao, F. (2019). Towards big data governance in cybersecurity. *Data-Enabled Discovery and Applications*, *3*(1). https://doi.org/10.1007/s41688-019-0034-9

Yeong Kim, H., & Suh Cho, J. (2018). Data governance framework for big data implementation with NPS case analysis in Korea. *Journal of Business & Retail Management Research*, *12*(03). 36-45. https://doi.org/10.24052/jbrmr/v12is03/art-04

Yin, R. K. (2017). *Case study research and applications: Design and methods*. SAGE.

Yost, J. R. (2016). The march of IDES: Early history of Intrusion-Detection Expert Systems. *IEEE Annals of the History of Computing*, *38*(4), 42–54. https://doi.org/10.1109/MAHC.2015.41

Young, J. C., Rose, D. C., Mumby, H. S., Benitez□Capistros, F., Derrick, C. J., Finch, T., Garcia, C., Home, C., Marwaha, E., Morgans, C., Parkinson, S., Shah, J., Wilson, K. A., & Mukherjee, N. (2018). A methodological guide to using and reporting on interviews in conservation science research. *Methods in Ecology and Evolution, 9*(1), 10-19. https://doi.org/10.1111/2041-210x.12828

Young, N., & Drees, R. (2018). Cybersecurity for automatic test equipment. *IEEE Instrumentation & Measurement Magazine, 21*(4), 4-8. https://doi.org/10.1109/MIM.2018.8423738

Zafar, H., Ko, M. S., & Osei-Bryson, K.-M. (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. https://doi.org/10.1007/s10796-015-9562-5

Zhang, X., Yuan, Y., Zhou, Z., Li, S., Qi, L., & Puthal, D. (2019). Intrusion Detection and Prevention in Cloud, Fog, and Internet of Things. *Security and Communications Network,* 2019(4529957), 1-4.

Appendix: Interview Protocol

Project: Walden University Doctorate of Information Technology Study

Type of Interview:____

Date:____

Place:____

Interviewer:____

Interviewee:____

Position Title of Interviewee:____

[Explain the project by clarifying about the (a) study purpose, (b) several sources of data collection, (c) confidentiality of data, and (d) conclusion of the interview in 60 minutes time.]

[Give contact information to the interviewee]

[Inform the interviewee about the consent form expected of all study participants, and about plans to record the interview audio (provide copy if necessary).]

[Test the digital audio recorder device for functionality. Confirm whether the participant agrees to session recording]

Interview Questions:

1. How do you evaluate data breaches in your organization, in terms of whether the organization is succeeding to contain them or it is spiraling out of control?

2. Between internal and external data breaches, which ones affect your organization the most and why?

3. Which strategies do you use to ensure your IT staff are qualified to address security breaches? Why or why not.

4. Which strategies do you employ to ensure adequate budgets for your IT department to address data breaches? Why or why not?department to address data breaches? Why or why not?

5. Explain whether your organization creates security awareness for employees through special programs implemented by the IS manager?

6. What procedures does your organization implement to conduct internal compliance audits as part of strategies used to protect information from cyberattacks?

7. What data safety processes does your organization implement to guard against unauthorized access to the organization's networks?

8. How often does your organization train their staff about the best practices for IT security? Do you think this is enough and why?

9. What is the extent of process automation in your organization as far as strategies used to protect information from cyberattacks are concerned?

10. How often does your organization periodically discard personal information at their disposal that they no longer require as part of their strategy to protect information from cyberattacks?

11. What are the procedures adopted by your organization in discarding personal information that is no longer required, in protecting information against cyberattacks?

12. Which strategies do you feel your organization should adopt to enhance IT security?

[Express gratitude to the interviewees for getting involved and assisting in the interview. Restate the study’s obscurity of the respondent and their responses. Notify the interviewee that you will provide them with the transcription file copy for assessment, consent, and return].