2022

Exploration of Cybersecurity Managers' Experiences Protecting Users' Privacy

Emmanuel Abayomi Segun
Walden University

Walden University

College of Management and Human Potential

This is to certify that the doctoral dissertation by

Emmanuel Abayomi Segun

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. Danielle Wright-Babb, Committee Chairperson, Management Faculty
Dr. Robert Haussmann, Committee Member, Management Faculty
Dr. Hamid Kazeroony, University Reviewer, Management Faculty

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

Walden University
2022

Abstract

Exploration of Cybersecurity Managers' Experiences Protecting Users' Privacy

by

Emmanuel Abayomi Segun

MPhil, Walden University, 2019

MSc, Johns Hopkins University, 2002

BS (HND), The Polytechnic, Ibadan, 1985

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Management

Walden University

May 2022

Abstract

The protection of individual privacy and personal data in cyberspace continues to be a problem. The research problem was that cybersecurity managers must constantly navigate between the adoption of new security laws, new applications, and the internet of things (IoT) to protect the privacy of individual users. The purpose of this descriptive phenomenological study was to explore the lived experiences of cybersecurity managers who have adopted new security laws, new applications, and the IoT to protect users' privacy. The conceptual framework that grounded this study was protection motivation theory and cybersecurity awareness. Data were collected through telephone and web based interviews with 16 purposefully selected cybersecurity managers. Thematic coding and categorization through NVivo software yielded themes about the protection of users' privacy and their adoption. The five major themes that emerged from my analysis of data were data security laws and the protection of users' privacy; new application by IoT affects users' privacy protection; the security of IoT devices is essential for IoT adoption; zero-day vulnerability and users' privacy protection; and continuous training is critical to cybersecurity awareness, privacy, and data protection. The findings of this study may have implications for positive social change by leading educational institutions to increase the knowledge of internet users, business managers to protect data and privacy, and governments to legislate appropriate laws to aid in the protection of personal data and individual users' privacy in cyberspace.

Exploration of Cybersecurity Managers' Experiences Protecting Users' Privacy

by

Emmanuel Abayomi Segun

MPhil, Walden University, 2019

MSc, Johns Hopkins, 2002

BS (HND), The Polytechnic, Ibadan, 1985

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Management

Walden University

May 2022

Dedication

I dedicate this work to the affectionate memory of my parents, Mr. Israel Abimbola Segun and Mrs. Matilda Olufunmilayo Segun, who laid the foundation for the zeal to embark on this journey and the resilience to follow through till the end.

Acknowledgments

I thank my Heavenly Father and my Lord who gave me the revelation to embark on this journey and for seeing me through all the pitfalls along the way. Sincere thanks and appreciation to my committee chair, Dr. Danielle Babb; committee member, Dr. Robert Haussmann; and URR Dr. Hamid Kazeroony for staying with me in the trenches until the very end. Notably, to Dr. Babb for her guidance and for ensuring I did not quit when I was ready to end it all, to Dr. Haussmann for his invaluable guidance at each critical stage along the way, and to Dr. Kazeroony for positively stretching me and tirelessly working with me to accelerate my movement to the finish line. To the three of you, I am exceedingly grateful for making this journey memorable. A sincere thank you to my first mentor, Dr. Walter McCollum, who guided me through the early part of the program, and Dr. Richard Hay, my academic adviser, whose incessant phone calls to check on me and his great advice kept me focused and on the right path. A very warm thank you and appreciation to my wife Clarissa, for her patience, understanding, long suffering, and steadfast encouragement from the beginning till the end. There is no way I could have finished without you by my side, and I am eternally grateful to you Sweetie. We did it; you did not marry a quitter as you would always say. I am forever grateful to everyone who contributed to the successful completion of this academic endeavor. Many of you were there to listen, stepped up to help when needed, and offered words of encouragement. I am exceedingly grateful for your support.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction to the Study

Introduction

As a result of theft and unauthorized and manipulative use of personal data, interest has increased in the issue of protecting personal data in cyberspace (Atkinson et al., 2009; Johansson & Gotestam, 2004; Pizzolante et al., 2018; Rahim et al., 2015; Sanchez Alcon et al., 2013). The protection of individual privacy online relies on the effective management and protection of personal data by cybersecurity managers. Equally important are individuals' privacy rights that have become eroded online (Brimblecombe, 2020). As a result, cybersecurity managers must constantly navigate between the adoption of new security laws, new applications, the IoT and the expanding landscape of technology to protect the privacy of individual users in cyberspace (Brimblecombe, 2020; Pizzolante et al., 2018; Sanchez Alcon et al., 2013).

The collection of individuals' personal information online has increased due to the expansion of the IoT, the behavior of individual users, and the introduction of smart devices, new applications and services (Lu et al., 2015; Öğütçü et al., 2016; Pizzolante et al., 2018; Sanchez Alcon, et al., 2013; Zhang, et al., 2019;). Despite the layers of information security mechanisms in place, human factors, including the behaviors of individual users, may affect the protection of privacy and personal data in cyberspace (Öğütçü et al., 2016). The study of the lived experiences of cybersecurity managers in the aforementioned areas would yield valuable data to aid in the development of cybersecurity policies and strategies. This chapter provides the background, the research problem statement, the purpose statement, the research question, the conceptual

framework, the research design, a listing of key terms, the study limitations, and a chapter summary.

Background of the Study

A systematic review of relevant literature revealed the problem inherent in navigating between the adoption of new security laws, new applications, and the IoT to protect the privacy of individual users by cybersecurity managers (Pizzolante et al., 2018; Sanchez Alcon et al., 2013). In addition, cybersecurity managers struggle with the problem of identifying what constitutes privacy in the IoT (Brimblecombe, 2020; Zhang et al., 2019). The online privacy of individual users is closely related to the protection and management of their personal data in cyberspace. Cybersecurity managers' understanding of what constitutes privacy of individuals in the emerging IoT will enhance their protection of users' privacy in cyberspace.

The IoT and the development of new applications has introduced serious privacy and security threats to individuals in cyberspace (Fawaz & Shin, 2019). Compounding the problem is the number of end user connected devices in the IoT that may reach "tens of billions" and even "trillion and beyond" as the adoption of IoT increases (Fawaz & Shin, 2019, p. 40; Ullah et al., 2018, p. 73468). With the IoT enabling new applications and interactions among interconnected devices, more challenges have been introduced for cybersecurity managers in protecting users' privacy and their connected devices from cyberthreats. Compounding this problem further is the differences in the behavior of the individual users whose privacy cybersecurity managers are supposed to protect. A review of literature on cybersecurity awareness revealed differences in internet users and

confirmed that younger internet users are the most vulnerable in cyberspace. Younger internet users share their personal data in cyberspace without observing cybersecurity. Cybersecurity managers may experience difficulty protecting the individual privacy of these users. No research has been conducted to investigate how cybersecurity managers could effectively protect the individual privacy of younger internet users concerning cybersecurity awareness, personal data protection, individual privacy, and identity theft. The findings of such research could yield future study directions concerning cybersecurity, protection of individual privacy, personal data, and identity theft for this group of internet users (Rahim et al., 2015).

A review of the literature also revealed several misalignments in the levels of cybersecurity knowledge and awareness among the population of youth internet users. Increased cybersecurity awareness may offer important defense in the protection of systems and the privacy of individuals in cyberspace. Targeted cybersecurity awareness campaigns that could address the weaknesses of specific populations of internet users may be necessary to facilitate the protection of individual privacy by cybersecurity managers. The research may yield additional knowledge that may help address some of the weaknesses in the online behaviors of individual internet users (Chandarman & Van Niekerk, 2017).

Another problem that may hinder the protection of individual privacy online by cybersecurity managers may be adolescents' excessive use of the internet, which can create cyberspace vulnerabilities like identity theft and online fraud. Research data on the security knowledge and skills of the youth population reveal most adolescents have

shared personal information online without any regard for data protection and security, which aligns with Rahim et al.'s (2015) findings. A review of literature confirmed that lack of restraint in sharing personal information is the riskiest activity among the adolescent population online. The findings of this study underscore the need for additional research to further understand the personal data protection and security needs of youth and adult internet users, so that cybersecurity managers can effectively protect their individual privacy online (Sithira & Nguwi, 2014).

Also relevant is the investigation into the relationship between organizational information security culture and employees' security behavior through the review of information security culture studies published in six leading databases from 2000 through 2016. Researchers focused on employee information security behavior and provided information on guidelines to improve employees' information security behavior. The behavior of internet users could have a corresponding effect on the protection of individual privacy online by cybersecurity managers. Akhyari et al. (2018) revealed a lack of comprehensive empirical studies that could provide sufficient empirical findings to support the relationship between employee information security behavior and information security organizational culture.

The use of different kinds of information and communications technology (ICT) has put the personal information of school learners at risk, and many school learners lack knowledge for the proper use of ICTs. A cyber-culture approach is needed to educate school learners and all role players (i.e., parents, teachers, and governments) about the culture of cyber-safety awareness. A lack of understanding of cyber-safety by school

learners could lead to reckless sharing of personal data, which cybercriminals could exploit in cyberspace. The reckless sharing of personal data without considering cybersecurity could make the protection of the privacy of individuals difficult for cybersecurity managers. Consequently, school learners using ICTs must understand cyber-safety risks when in cyberspace and must have adequate knowledge about the identification of cyber-safety risks to mitigate and prevent them (Kritzinger (2017).

The behavior of internet users could also affect the protection of their individual privacy in cyberspace. Risky behavior of users, which is closely related to their information security awareness, could lead to threat exposure that could compound the protection of the privacy of individuals by cybersecurity managers in cyberspace. Users are the biggest threat to information security as they represent the weakest link in an information security defensive armor (Öğütçü et al. (2016). These weak links, who could be unsuspecting information systems users, are now being exploited by cybercriminals who have shifted their focus from information technology components to attacking organizational networks through the exploitation of the vulnerability of unsuspecting information systems users (Abawajy, 2014)

Cybersecurity managers must constantly navigate between the adoption of new security laws, applications, and the IoT to protect the privacy of individuals in cyberspace (Pizzolante et al.; 2018; Sanchez Alcon et al., 2013). Equally discussed in the literature is the problem of identifying what constitutes privacy in the IoT by cybersecurity managers (Brimblecombe, 2020: Zhang et al., 2019). A lack of understanding of cyber-safety and information security awareness by internet users could lead to these users recklessly

sharing their personal data in cyberspace (Kritzinger 2017; Öğütçü et al., 2016). This behavior could negate the protection of individual privacy in cyberspace by cybersecurity managers. There has been little to no research conducted to study the lived experiences of cybersecurity managers concerning how they have navigated these areas of cybersecurity (Kritzinger, 2017; Pizzolante et al.; 2018; Sanchez Alcon et al., 2013). With this study, I sought to fill this gap in knowledge by exploring the lived experiences of cybersecurity managers regarding individual privacy in the United States concerning these specific areas of cybersecurity. The results of this research may provide additional knowledge in the field of cybersecurity.

Problem Statement

Cyberspace has become a platform for individual internet users to interact with one another, and users' personal data are often exploited by cybercriminals (Magolis & Briggs, 2016; Rahim et al., 2015). The protection of individual privacy, which is closely related to the protection and management of personal data, lies in the behavior of individual users and the management of personal data by cybersecurity managers. A recent survey by Pew Research confirmed that most Americans have little to no control over their personal data they share with organizations and governments and upload to online destinations (Auxier et al., 2019). Specifically, 81%–84% of Americans confirmed little to no control over their personal data with companies and government. A sizable number of Americans (81%–66%) confirmed that the risk of sharing their personal data with companies and governments outweighs the benefits. Equally, 79%–64% stated they had concern over the use of their data by companies and governments, and 59%–78%

confirmed lack of understanding on the use of their personal data by companies and governments. Within these prevailing user situations, cybersecurity managers still must find a way to navigate between the adoption of new data security laws, applications, and the IoT to protect the privacy of individual users in cyberspace (Pizzolante et al., 2018; Sanchez Alcon et al., 2013). The review of literature revealed a lack of comprehensive research studies conducted to provide sufficient findings in support of how cybersecurity managers should manage this situation. This problem represents a gap in literature that I sought to fill with this study.

The general management problem is that cybersecurity managers face the task of identifying what constitutes privacy in the IoT (Brimblecombe, 2020; Zhang et al., 2019). The specific management problem is that cybersecurity managers must constantly navigate between adoption of new security laws, new applications, and the IoT to protect the privacy of individual users (Pizzolante et al., 2018; Sanchez Alcon et al., 2013).

Purpose of the Study

The purpose of this descriptive phenomenological study was to explore the lived experiences of cybersecurity managers adopting new security laws, new applications, and the IoT to protect users' privacy in the metro areas of Washington D.C., Maryland, and northern Virginia. Data were collected through telephone and Zoom audio and video interviews with a purposefully selected sample of the study population using an interview protocol with open-ended questions. The data provide an opportunity to learn about the lived experiences of cybersecurity managers adopting new security laws, new applications, and the IoT to protect users' privacy.

Research Questions

The following research question guided this study: What are the lived experiences of cybersecurity managers adopting new security laws, new applications, and the IoT to protect users' privacy in the United States?

Conceptual Framework

The conceptual framework that grounds this study is Rogers' (1975, 1983) protection motivation theory (PMT) and cybersecurity awareness. Shillair et al. (2015) confirmed that PMT is a model of social cognitive theory, known as social learning theory (Bandura, 1986), and has been used to understand computer behavior. PMT has also been used as part of online safety protection research (Anderson & Agarwal, 2010; Johnston & Warkentin, 2010). An aspect of PMT relevant to the current study is the behavioral intentions of internet users (i.e., cybersecurity managers) who are the population of this study.

Rogers (1975, 1983) presented two appraisal methods in the PMT mediating processes: threat appraisals and coping appraisals. Individuals perform these two appraisals in the assessment of their need to engage in a behavior in response to a threat. These two appraisals are responsible for the behavioral intentions of internet users in adopting protective security intentions to protect themselves while interacting in cyberspace (Tsai et al., 2016). Internet users may engage in protective behaviors that could ensure the security of their personal data online. PMT provides a lens to view the study population concerning the protection of personal data and individual privacy as the

users interact in cyberspace. Further exploration of this theory will be part of the literature review in Chapter 2.

The protection of individual privacy is closely related to the protection of personal data in cyberspace, which may require cybersecurity awareness by the study population. Cybersecurity awareness focuses on the methodical way to educate internet users about cyberthreats and the vulnerability of data and computer systems to these threats (Rahim et al. 2015; Shaw et al. 2009). Personal data protection focuses on the protection of personal data from the invasion of cybercriminals in cyberspace (Broadhurst & Chang, 2013). The online behavior of internet users is a function of their knowledge of personal data protection and cybersecurity in cyberspace. Exploring personal data protection and cybersecurity from the lived experiences of the study participants could provide an understanding of the prevailing cybersecurity situation and the necessary actions to educate others.

Nature of the Study

The qualitative research design was selected for this study to allow collection of meaningful and reliable data from participants (Denzin & Lincoln, 2005; Kruth, 2015; Patton, 2015). Kruth (2015) posited that a qualitative research design allows for the exploration of different human experiences concerning events, phenomena, and different situations observed or experienced in normal environments. Qualitative methodology allows researchers to interact with study participants through face-to-face interviews, in person, virtually or via telephone, and focus groups. These methods of data collection

provide opportunities for immediate follow-up questions for necessary clarification of any unclear responses.

The selected qualitative research approach for this study was a phenomenological approach. This approach allows a researcher to conduct description and interpretation to yield understanding, individual growth, and progressive social knowledge (Slattery et al., 2007; van Manen, 2002). The phenomenological research approach is an in-depth inquiry into things as they appear, which leads to an essential understanding of human experience and consciousness (Dowling, 2007; Husserl, 1970; Moustakas, 1994; Valle et al., 1989). Hein and Austin (2001) supported the phenomenological research, stating that phenomenology involved "the systematic study of experience or human meaning" (p. 4), which can be studied rigorously from the perspective of how it appears to human experience and consciousness. Descriptive phenomenology, as used in this research, involves a focus on interpreting the essence of the lived experiences concerning a phenomenon to provide an in-depth understanding of the phenomenon.

The planned sample size for this research was between 15 and 20 participants. Qualitative research methodology provided the opportunity to ask open-ended questions from participants through in-depth interviews and guided the choice of sampling strategy and the collection of data. Purposeful sampling strategy, which aligns with the qualitative research methodology, was the selected sampling strategy for this study and was used to select information-rich cases from the study population. The final analysis of data through thematic coding and categorization of responses from participants was performed with NVivo qualitative data analysis (QDA) software.

Definitions

Cybersecurity: The gathering and organization of resources, processes, and structures used to protect cyber-enabled systems and cyberspace from intentional events designed to undermine the integrity and security of cyberspace (Craigen et al., 2014).

Cybersecurity awareness: The methodology of educating internet users to be aware of the various cyberthreats and the vulnerability of data and computer systems to these threats in cyberspace (Rahim et al. 2015; Shaw et al., 2009).

Cyberspace: A virtual global domain of interdependent and interconnected networks of information technology (IT) infrastructures, which includes computer systems with installed processors and controllers, the internet, and telecommunication networks (U.S. Cyberspace Policy Review, 2009).

Identity theft: The use of a person's personal data falsely through deceit and fraud specifically for economic gain (U.S. Department of Justice, 2011).

Personal data protection: The protection of individuals' personal data from treacherous invasion aimed explicitly at obtaining individuals' personal data for illegal use (Broadhurst & Chang, 2013). Personal data center on the "identifiability of a person … and the relation of information to a person" (Purtova, 2018, pp. 41–42). In the United States, the California Consumer Privacy Act defined personal information as "any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a consumer or household" (de la Torre 2018, p. 6). The definition specifically includes contact information, government IDs, biometrics, genetic data, location data, account numbers, education history, purchase

history, online and device IDs, and search and browsing history and other online activities if such information is linked or linkable with a particular consumer or household. Under the law, *consumer* is broadly defined as "any resident of California" (DLA Piper Intelligence, 2020). The European Union General Data Protection Regulation defined personal data as:

> Any information relating to an individual or identifiable natural person (e.g., data subject); an identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. (Purtova, 2018, p. 43)

These global definitions of personal data are applicable to the population of this research study. The protection of any of these data points could be referred to as privacy and personal data protection.

Assumptions

The first assumption was that the perspectives of the participants are essential, meaningful, and worthy of an explicit narrative. I assumed that participants would provide real and accurate responses to the interview questions. The second assumption was that participants would be savvy internet users who have experienced cybersecurity awareness, personal data, and privacy issues and would remember their lived experiences and be willing and ready to share them.

Also significant is the philosophical assumption for the study, which follows the constructivist tradition. This tradition sees the meaning of reality (ontology) as multiple and varied between groups of individuals; hence, researchers explore diverse experiences to avoid focusing on a few categories (Goduka, 2012). Based on this assumption, I expected that each participant would come with different lived experiences concerning privacy, personal data protection, and cybersecurity awareness. The different perspectives from participants would be captured during field interviews and analyzed for an adequate understanding of the study population concerning privacy, personal data protection, and cybersecurity.

Scope and Delimitations

The scope of this descriptive phenomenological study was limited to the examination of the lived experiences of cybersecurity managers in the United States, concerning the individual privacy protection and security of personal data, a subset of which is identity theft in cyberspace. An aspect of the research problem addressed in the study was the exploration of the online behavior of the study population and their protection of individual privacy as they interact in cyberspace. Atkinson et al. (2009), Johanson and Gotestam (2004), and Rahim et al. (2015) confirmed that the personal data of internet users is exploited in cyberspace by cybercriminals. This problem has increased as the study population must constantly navigate the adoption of new security laws, new applications, and the IoT to protect the privacy of users and their personal data in cyberspace (Pizzolante et al., 2018; Sanchez Alcon et al., 2013). PMT, provides an

understanding of the protective behaviors of internet users and cybersecurity awareness and was the conceptual framework for this descriptive phenomenological study.

Limitations

The study followed the qualitative research methodology, which may limit it due to the relative weaknesses of the method. The use of purposeful sampling to select research participants may have made study participants not adequately representative of the population. However, this did not impede the relevance of the study as purposeful random sampling (Patton, 2015) was used to mitigate this risk.

Research is only as good as the quality of data collected and analyzed for the corresponding findings. Collection of data in qualitative research can take place through many methods. Data were collected in this descriptive phenomenological study through interviews, which may have introduced some limitation to the study. The uniqueness and depth of experiential Knowledge of the cybersecurity participants interviewed would mitigate the weakness that may result from the use of interviews as the only data collection method.

My role as the researcher may introduce limitations to the research in terms of biases. Because I served as the instrument during the field interviews, I had to ensure there was no personal or professional relationship with study participants. I identified study participants and developed appropriate relationships with them but was cautious to guide against any form of bias. Participants may have come with preferences as well. I was conscious of the prejudices and ready to document and deliberately guide against them.

Significance of the Study

This descriptive phenomenological study may provide the opportunity to learn about the lived experiences of cybersecurity managers who are adopting new security laws, new applications, and the IoT to protect the privacy of individuals. This section covers three distinct areas: (a) the significance of the study to theory, (b) the study's significance to the practice of cybersecurity, and (c) the significance of the study to positive social change.

This research may contribute to filling a gap in the understanding of privacy, personal data protection and security in cyberspace. The study may provide salient data significant to theory through the exploration of the lived experiences of the study participants concerning cybersecurity and personal data protection. Data from the study could also shed light on further understanding of cyberspace and the security of the interconnected information technology assets.

This research could help improve the practice of cybersecurity and personal data protection and security concerning the target population. Studying this population may shed light on the different levels of cybersecurity awareness and understanding that they possess and the amount of help they may need in terms of cybersecurity (Chandarman & Van Niekerk, 2017). Data from this study could also facilitate the development of specific programmable instructions at different levels of understanding regarding data and cybersecurity.

The findings from this study could lead to positive social change by representing valuable research data that may be used to develop cybersecurity policies and strategies

aimed at protecting the privacy of internet users. Business managers could have more information on how best to protect data and privacy. Governments could have the opportunity to legislate appropriate laws that may protect internet users if needed. Educational institutions could also develop a relevant curriculum that may increase the understanding of internet users.

Summary and Transition

In this Chapter, I presented the background, the problem statement, the purpose, the research question, conceptual framework, nature of the study, definition of terms used, my assumption throughout the research, scope and limitations of the study, and the study's significance and how it might produce positive social change. Chapter 2 will contain the literature review.

Chapter 2: Literature Review

Introduction

The specific management problem is that cybersecurity managers must constantly navigate between adoption of new security laws, new applications, and the IoT to protect the privacy of individual users (Pizzolante et al., 2018; Sanchez Alcon et al., 2013). The purpose of this descriptive phenomenological study was to explore the lived experiences of cybersecurity managers adopting new security laws, new applications, and the IoT to protect individuals' privacy in the metro areas of Washington D.C., Maryland, and northern Virginia. Data were collected through telephone and Zoom video interviews with a purposefully selected sample of the study population using an interview protocol with open-ended questions. The study findings may provide information about the lived experiences of cybersecurity managers adopting new security laws, new applications, and the IoT to protect individual privacy.

In this literature review, I provide a look at the seminal writings of Rogers (1975, 1983) on PMT and discuss how the behavioral intentions of the study population could be viewed through the lens of this theory. I describe the constructs of interest and justification for the chosen methodology and approach consistent with the scope of this descriptive phenomenological study. I present qualitative research methodology as the preferred research methodology and look at the works of Heidegger (1889–1976) and Gadamer (1900–2002) with other philosophers on descriptive phenomenology, which was the approach for this descriptive phenomenological study. Concepts of interest

central to the scope of the study are cybersecurity awareness and personal data protection; I review and synthesize studies related to these key concepts.

Literature Search Strategy

The literature search was conducted using Google, Google Scholar, ProQuest Central, Academic Search Complete, Science Direct, EBSCOhost, ABI/Inform Global, the Walden University library, and recent Walden dissertations. Search terms included *privacy, security, applications, and the IoT, adoption of security and privacy in the IoT, protection motivation theory (PMT), behavioral intention, social cognitive theory, Albert Bandura, phenomenology, descriptive phenomenology, Edmund Husserl, Maurice Merleau-Ponty, Amadeo Giorgi, lived experience, cybersecurity awareness, protection of personal data among adults and youth, identity theft,* and *cyberspace*. A search of EBSCOhost for documents relating to privacy, security, and IoT on October 17, 2020, yielded 366 peer-reviewed articles. A search of Business Source Complete for documents relating to descriptive phenomenology on the same date yielded 57 peer-reviewed articles. A search of ABI/Inform Global for documents relating to the adoption of security and privacy in the IoT on October 21, 2020, yielded 20 peer-reviewed articles. A search of Google Scholar for documents relating to phenomenology on April 10, 2020, yielded 1,260,000 documents, of which 26,000 were published between 2018 and 2020. The search for descriptive phenomenology published in the same timeframe yielded 20,900 documents. A search for cybersecurity yielded 50,000 documents, of which 6,620 were on youth and cybersecurity. A joint search for protection motivation theory, data protection, and security in Google Scholar yielded 16,800 documents in the above-

mentioned timeframe. A search for documents on cybersecurity awareness among cybersecurity managers yielded 29,000 results of which 22,300 were from 2016 to November 30, 2020. ProQuest Central dissertation search on personal data protection and cybersecurity yielded 359 dissertations.

Further searches in Google Scholar yielded salient contents purposefully selected based on their relevance to the current study; the following keywords were used: *qualitative, descriptive, transcendental, existential, lived experience, phenomenological qualitative research, and descriptive phenomenology as a research method*. Articles were further verified through Ulreich to ensure they were peer reviewed. The literature review includes 150 articles, of which 125 (83.3%) were peer reviewed and 138 (92%) were published within 5 years of expected chief academic officer approval of this study. In the literature, I reviewed the conceptual framework, which is PMT and cybersecurity awareness, their contextual relevance, and how they apply to the research study. Discussion also focuses on the supporting concept of cybersecurity awareness. Included in the discussion are studies in which researchers used PMT, cybersecurity awareness, and the qualitative research methodology.

Conceptual Framework

The conceptual framework that grounded this study was Rogers' (1975, 1983) PMT and cybersecurity awareness. Shillair et al. (2015) confirmed that PMT is a model of social cognitive theory, known as social learning theory (Bandura, 1986). Shillair et al. confirmed that PMT has been used to understand computer behavior. PMT's usage was also part of the online safety protection study, according to Anderson and Agarwal (2010)

and Johnston and Warkentin (2010), and, hence, the theory I chose for this study. An aspect of PMT relevant to the current study is the behavioral intentions of internet users (i.e., cybersecurity managers), who are the population of this study.

Rogers presented two appraisal methods in PMT mediating processes: threat appraisals and coping appraisals. Individuals perform these two appraisals in the assessment of their need to engage in a behavior in response to a threat. These two appraisals are responsible for the behavioral intentions of internet users in adopting protective security intentions to protect themselves while interacting in cyberspace (Tsai et al., 2016). Internet users may engage in protective behaviors that could ensure the security of their personal data online. PMT provides a lens to view the study population concerning the protection of personal data and individual privacy as they interact in cyberspace.

Protection of individual privacy is closely related to protection of personal data in cyberspace. This may require an awareness of cybersecurity by the study population. Cybersecurity awareness focuses on the methodical way to educate internet users about cyberthreats and the vulnerability of data and computer systems to these threats (Rahim et al. 2015; Shaw et al.2009). Personal data protection focuses on the protection of personal data from the invasion of cybercriminals in cyberspace (Broadhurst & Chang, 2013). The online behavior of internet users is a function of their knowledge of personal data protection and cybersecurity in cyberspace. Exploring personal data protection and cybersecurity from the lived experiences of the study participants could provide an

understanding of the prevailing cybersecurity situation and the necessary actions to educate others.

Literature Review

A systematic review of relevant literature revealed the problem inherent in navigating between the adoption of new security laws, new applications, and the IoT to protect the privacy of individual users by cybersecurity managers (Pizzolante et al., 2018; Sanchez Alcon et al., 2013). There is also a problem regarding the identification of what constitutes privacy in the IoT by cybersecurity managers (Brimblecombe, 2020; Zhang et al., 2019). The online privacy of individual users is closely related to the protection and management of their personal data in cyberspace. Cybersecurity managers' understanding of what constitutes privacy of individuals in the emerging IoT will enhance their protection of users' privacy in cyberspace.

The IoT, with the accompanying development of new applications, has introduced privacy and security threats in cyberspace (Fawaz & Shin, 2019). Compounding the problem is the number of end user connected devices in the IoT that may reach "tens of billions" and even "trillion and beyond" as the adoption of IoT increases (Fawaz & Shin, 2019, p. 40; Ullah et al., 2018, p. 73468). New applications enabled by IoT and the interactions among interconnected devices have introduced more challenges for cybersecurity managers in protecting users' privacy and their connected devices from the prevailing cyberthreats. Enhancing the privacy capabilities of multiaccess edge computing (MEC) in IoT systems could be a solution to these challenges.

MEC enhances the security and privacy of the networks of IoT systems, as communication takes place among IoT devices and remote servers (Zhang et al., 2019). Consequently, MEC can facilitate protecting the privacy of individuals whose personal data move across IoT devices. IoT has the potential to become the next biggest innovation after the emergence and full adoption of the internet (Zhang, et al., 2019). The things in the IoT are comprised of different types of devices that process and store genomic information, hence the term *internet of living things* (Pizzolante et al., 2018).

The interconnectedness of several mobile and stationary devices (e.g., personal electronics, office equipment, house appliances, public infrastructure, and ubiquitous sensors; Zhang et al., 2019, p. 730) together with smart applications (e.g., smart cars, smart homes, smart cities, etc.) may enhance the quality of human lives. However, the networks of these smart devices and applications could create accompanying challenges concerning the protection of individual users' privacy in cyberspace. This is because this interconnectedness may allow personal data to fall into the hands of opportunistic individuals. Cybersecurity managers may be able to resolve privacy challenges among cyber-connected devices in IoT through MEC, sequencing sensors, and utility matrix (Pizzolante et al., 2018; Sanchez Alcon et al., 2013; Zhang et al., 2019). Another key area of concern to cybersecurity managers is new security laws.

Data security laws are enacted to protect people's personal information. The protection of individual privacy in cyberspace depends on the protection and effective management of individuals' personal data. Personal data are centered on the "identifiability of a person … and the relation of information to a person" (Purtova, 2018,

pp. 41–42). Personal information refers to “any information that identifies, relates to, describes, or is capable of being associated with, a particular individual” (de la Torre, 2018, p. 6). This quoted description of personal information from the California Consumer Privacy Act is in alignment with the European Union’s (EU) depiction of personal data in the General Data Protection Regulation law of 2018. The EU data protection law describes personal data as “any information relating to an identified or identifiable natural person … referred to as ‘data subject’” (de la Torre, 2018, p. 6). Despite the EU’s attempt to enact a law to protect the privacy of individuals, Purtova (2018) argued that the personal data of individuals will continue to grow, and its application could expand to an array of diverse meaning and interpretation. Consequently, the emerging changing interpretation of the concept of personal information in the IoT due to the “exploding generation and aggregation of data, as well as advances in data analytics” (Purtova, p. 41) could make the protection of individuals’ privacy by cybersecurity managers difficult in cyberspace.

Another development concerning personal data is the public interest in deleted personal data that emanates from the “right to erasure… otherwise known as the right to be forgotten” (Brimblecombe, 2020, p. 9). The right provides individuals with the legal authority, in some situations, to request the deletion of their personal data from online destinations. All the same, the significance of the privacy provided by this right to individuals remains unclear (Brimblecombe, 2020).

Privacy-enhancing security services should be built into products and solutions that make up the IoT. As the interconnectedness of new smart devices and applications

within the IoT continues to increase in accelerated dimensions, there is a need to build security services that enhance confidentiality, integrity, and availability. Examples of such products are “accessible wearable device platform for smart environments” (Sanchez Alcon et al., 2013, p. 72). These products provide physiological monitoring capabilities that enhance the remote inspection and monitoring of the status of peoples’ health in different locations. The products also provide real-time actionable data to health professionals. Within the IoT is the internet of living things, which are “networks of biological sequencing sensors” (Pizzolante et al., 2018, p. 384). The internet of living things was built through networks of devices used for DNA arrangement and analysis. Of concern to cybersecurity managers is the protection of the privacy of individuals whose health data are transmitted through these devices (Pizzolante et al., 2018; Sanchez Alcon et al., 2013).

Additionally, cybersecurity managers are likely concerned regarding the misalignment in the levels of cybersecurity knowledge and awareness of the people whose privacy needs are to be protected. Cybersecurity awareness offers an important defense in the protection of systems and people. The misalignment in the levels of cybersecurity knowledge and awareness of individual users could call for cybersecurity awareness campaigns to address the cybersecurity weaknesses of people (Chandarman & Van Niekerk, 2017). Individual user privacy erosion due to the use of ICTs is another major concern to cybersecurity managers.

ICTs are among the networks of interconnected devices that constitute the IoT in cyberspace. The use of these ICTs has led to the erosion of the privacy of individual

users, the majority of whom were school learners (Kritzinger, 2017). Review of literature revealed that school learners lack the necessary knowledge for the proper use of ICTs, due to lack of understanding of cyber-safety. The lack of cyber-safety could lead to the reckless sharing of personal data in cyberspace for cybercriminals to exploit. Consequently, Kritzinger (2017) asserted that it may be necessary to educate school learners and all role players (i.e., parents, teachers, and governments) about cyber-safety awareness. The education could provide school learners and all role players with adequate knowledge about the identification of cyber-safety risks so that they are able to mitigate and prevent them. It also enhances the protection of individual privacy of these internet users by cybersecurity managers (Fawaz & Shin, 2019; Kritzinger; Ullah et al., 2018). Equally important is the behavior of internet users.

The behavior of internet users could also affect the protection of their individual privacy in cyberspace. The reason being that the personal information security risky behavior of users, which is closely related to their information security awareness, could lead to threat exposure that could compound the protection of the privacy of individuals by cybersecurity managers in cyberspace. The review of literature revealed that users are the biggest threat to information security as they represent the weakest link in an information security defensive armor (Öğütçü et al. 2016). These weak links, who could be unsuspecting information systems users, are now being exploited by cybercriminals who have shifted their focus from information technology components to attacking organizational networks through the exploitation of the vulnerability of unsuspecting information systems users (Abawajy, 2014).

The systematic review of literature has revealed that cybersecurity managers face the problem of constantly navigating between the adoption of new security laws, applications, and the IoT to protect the privacy of individuals in cyberspace (Pizzolante et al.; 2018; Sanchez Alcon et al., 2013). Equally discussed is the problem of identifying what constitutes privacy in the IoT by cybersecurity managers (Brimblecombe, 2020: Zhang et al., 2019). Compounding the problems further, is the lack of understanding of cyber-safety and information security awareness by internet users who could recklessly share their personal data in cyberspace (Kritzinger 2017; Öğütçü et al., 2016). This behavior could negate the protection of individual privacy in cyberspace by cybersecurity managers. There has been little to no research that has specifically studied the lived experiences of cybersecurity managers concerning how they have navigated these areas of cybersecurity (Kritzinger, 2017; Pizzolante et al.; 2018; Sanchez Alcon et al., 2013). This is a gap in knowledge that I will aim to fill with this study. It is therefore necessary to study the lived experiences of cybersecurity managers on individual privacy in the United States concerning these specific areas of cybersecurity. The result of the research may yield new research data that could provide additional knowledge in the field of cybersecurity. A discussion that focuses on PMT will now follow.

Protection Motivation Theory

An aspect of the PMT (Rogers, 1975, 1983) that is relevant to this descriptive phenomenological study is the behavioral intentions of internet users who are among the population of this descriptive phenomenological study. The PMT provides a lens to view the study population concerning how they protect the privacy and personal data of

internet users in cyberspace. Shillair et al. (2015) explained that there is semblance in protecting one's health and protecting one's computer. The same protection could extend to an individual's online behavior concerning what is shared while using any means of ICT. Although the PMT has been a well-known approach used in health communication, it has also been used in studies regarding online safety protection (Anderson & Agarwal, 2010; Johnston & Warkentin, 2010; Shillair et al.; Siponen et al., 2014; Tsai et al., 2016). Rogers (1975, 1983) presented two appraisal methods in the PMT cognitive mediating processes: threat and coping appraisals. Individuals perform these two appraisals in their assessment of their need to engage in a behavior in response to a threat. Tsai et al. (2016) posited that both appraisals are responsible for the behavioral intentions of internet users, in adopting protective security intentions, to protect themselves while interacting in cyberspace. In response to a threat, like the online lure for internet users to share their personal data, the PMT posited that individuals engage in a behavior that could be adaptive or maladaptive. Adaptive responses are effective in protecting an individual while responding to a threat; maladaptive responses occur when an individual decides to either do nothing or do something that increases risks. This could be the unguarded sharing of personally identifiable information (PII) online without caution or opening email attachments from unknown sources. Therefore, in the process of completing a threat appraisal, the PMT explained that an individual cognitively assesses exposure and vulnerability to the threat and then develops an adaptive response. The adaptive response is referred to as coping self-efficacy, which occurs when an individual assesses how to respond positively to a threat. The second is the likelihood that the adaptive response

would be an effective deterrence to the threat. This is known as the coping response efficacy. Equally important is the inherent reward, which influences an individual to perform a protective behavior, and the associated perceived costs of adopting such a protective behavior. Rogers (1983) stated that such costs could be "inconvenience, expense, unpleasantness, difficulty, complexity, side effects, disruption of daily life …" (p. 169). Using inconvenience as an example, the cost could be the inconvenience of not taking part in an online event because it could expose a person to various forms of online vulnerabilities. Other costs could be the disruption of a person's daily life, or the unpleasantness of not joining an online group, because of an unwillingness to share certain requested personal information considered to be too intrusive. The second appraisal method in the PMT cognitive mediating processes is the coping appraisal method.

Rogers (1983) posited that the coping appraisal process helps individuals in evaluating their ability to cope with a threatening danger to avert it. It is the belief that the coping response is effective enough to avoid the danger associated with the threat (e.g., the belief that not sharing personal information will prevent cybercriminals from harvesting personal information in cyberspace). Shillair et al. (2015) explained that coping appraisal emanates from response efficacy beliefs, which focuses on the effectiveness of adaptive responses in resolving threats. Efficacy refers to the ability to produce an intended result, and it leads to the concept of self-efficacy that is important to the PMT.

Self-efficacy was not part of the original version of the PMT. It is a new component that was added later as part of the revised theory of protection motivation (Rogers, 1983). Self-efficacy refers to an individual's mastery and ability to produce a desired result. It is the belief that an individual could successfully perform the adaptive response to mitigate a threat. Bandura (1977) confirmed the importance of self-efficacy and explained that the mediation of the processes of psychological change depends on changes to the self-efficacy senses of individuals. Bandura believed that the determination on the initiation of coping behavior and the choosing of a behavior out of available behaviors is dependent on an individual's cognitive appraisal of self-efficacy concerning the threat. The determination on the amount of effort to expend, and the duration of effort considering inherent obstacles, is also dependent on a person's cognitive appraisal of self-efficacy about the threat.

As previously discussed, the concepts of the PMT are applicable to internet users who must make sense of risky online behaviors, such as deciding what information to share, as they are bombarded with online requests for personal data on daily basis. Internet users need to know that there is a threat in cyberspace concerning their personal data and they must be able to take protective actions to protect their personal data. Taking into consideration the discrepancy between realizing online threats and taking protective actions that emanate from adequate cybersecurity awareness, the current study uses PMT as the conceptual background. PMT helps to understand what drives the online safety behavior of internet users, who are within the population of this qualitative

phenomenological study, concerning the protection of their individual privacy and personal data in cyberspace.

Use of Protection Motivation Theory in Studies

Shillair et al. (2015) explored the motivation of internet users concerning their mental processes in following safe practices when they interact in cyberspace and suggested that internet users still do not follow safety precautions and consequently open themselves, the computer, and networks through which they connect, to various forms of vulnerabilities. Shillair et al. believed that the individual user is the key factor in cybersecurity. Despite the activities of online predators, many internet users still share their personal data online, affording cybercriminals the opportunity to harvest readily available personal information. Rainie et al. (2013) provided a succinct example in the recent Pew Research Center Survey of the amount of personal data internet users share online. The survey revealed that almost two-thirds of internet users post their photos publicly online, 50% confirmed that they have shared their year of birth, and 46% confirmed that they have shared their email address online. The survey also found that 44% have shared the name of their employer online, 38% confirmed that they have shared their writings using their real name, and 30% have shared their home addresses online. These behaviors deserve further exploration, hence understanding the behavioral intentions of internet users are important so that cybersecurity managers can protect their individual privacy online. Shillair et al. selected the PMT that belongs to the class of the social cognitive theory as the theoretical foundation, because it provides an understanding

of behavioral intentions. Shillair et al. extended PMT to the social-cognitive approach, which enhances the understanding of online safety behaviors.

In response to persuasive messages, Shillair et al. (2015) hypothesized the constructs of the PMT that are (a) coping self-efficacy and (b) intentions to engage in self-protective behavior, which would increase because of the vicarious experience of enactive mastery. The other three hypotheses in the study focused on internet users' personal responsibility. One was that internet users with higher personal responsibility would more likely engage in protective behavior. Another was that the level of personal responsibility would moderate the level of interventions strategy. The other was that personal responsibility norms and coping self-efficacy would be positively related to internet users' considerations to engage in protective behavioral intentions.

Shillair et al. (2015) recruited participants using a commercial mailing list vendor that provided a random sampling of households. Participants received an initial mailing that included the purpose of the study and their rights as human subjects. A follow-up letter provided the log-in ID to the online survey questionnaire and information about a nominal cash incentive for taking part in the survey. There were 2,000 mail solicitations sent out; 109 (approximately 5%) were undeliverable due to bad addresses, which left a usable recruitment count of 1,891. Participants who responded to the survey numbered 436, of which 161 were internet users and 280 were not internet users. As a result, there are 161 participants for the study. The data analysis method included the use of a 7-point Likert-type scale for dependent variable assessments. Data analysis also included model measurement, factor analysis, and the testing of hypotheses. Some of the PMT

hypotheses tested were confirmed while others were not. There was a significant effect on coping self-efficacy, as internet users who had vicarious treatment experiences, had higher levels of coping self-efficacy. This was the same for those with prior knowledge of online safety problems. However, the effect of personal responsibility on condition concerning safety behavioral intentions was not significant at the higher level of prior knowledge. All the same, the effect of personal responsibility at the lower level of prior knowledge among internet users increased safety intentions.

Posey et al. (2014) used the PMT as the theoretical foundation to explore the perception of organizational insiders and organizational security efforts conducted by organizations' security professionals. Since the behavioral intentions of organizational insiders' influence security efforts effectiveness, there was the need to study the mindset of insiders concerning the relationship they had with information security efforts. The mindset was then compared against the mindset of informational security professionals. Posey et al. noted a lack of research regarding the perception of organizational insiders concerning information security. The perception of organizational insiders concerning information security was compared to the perception of information security professionals. The focus concerning information security has always been on the technical methods, by information security professionals, instead of focusing on the online behavioral intentions of organizational insiders.

To study the difference in the perception of the two groups, Posey et al. (2014) recruited participants from various industry groups. The group included academic forum boards and organizational information security professionals. Posey et al. used the

qualitative research methodology in gathering data from study participants and designed interview protocol based on open-ended questions from past protection motivation research. Posey et al. conducted a total of 33 semistructured 30-minute phone interviews; 22 of whom were organizational insiders and 11 of whom were information security professionals. All participants provided approval for the recording of interviews based on assurance from the researchers that responses would be confidential. Transcription of interview data followed all interviews and Posey et al. used NVivo 8 data analysis program to analyze the contents of all interviews. Themes from the interview data formed the basis of thematic analysis that started with the coding of data, counting, and grouping, of common themes, which emanated from participants' responses to the PMT interview questions components.

Posey et al (2014) found that the prevalent security concerns of organizational insiders were hackers (39%) and internet threats (22%). Issues with hackers and internet threats were the top two information security threats. Themes from security professionals' responses showed similar and dissimilar concerns regarding security threats in comparison to the data from organizational insiders. Dissimilarly, response data from security professionals revealed differences in employee threats in contrast to data from insiders. Security professionals returned data that showed intentional and unintentional employee threats that were 22% and 35%, respectively, as a major concern. The themes that showed the largest contrast were hacker threats. A small percentage (4%) of security professionals considered hackers as threats, whereas 39% of the themes from insiders considered hackers as a threat to information security. This difference is

significant and should guide organizations in making informed policy decisions with respect to organizational information security.

Tsai et al. (2016) conducted a research study to examine the classical and the new PMT factors, to understand how they predict security intentions. Tsai et al. indicated that internet users still experience various forms of online safety threats requiring further safety precautionary methods. The authors reviewed ongoing research in online safety behavior and added the motivational factors in the studies to the PMT framework to examine how internet users engage in coping and threat appraisals, which are major components of the PMT.

Tsai et al. (2016) conducted an online survey using Amazon's Mechanical Turk (MTurk), which is a large recruiting workforce sourcing platform. Tsai et al. confirmed through other research that MTurk was more representative of the population of the United States and recruited 988 participants who have 90% human intelligence task (HIT) approval rates. The HIT approval rate represents professionalism, and its determination comes from the total number of approved and recorded worker assignments. The authors believed that the use of the 90% HIT approval rating was arbitrary but confirmed the rate has been used in other cited research studies. Tsai et al. noted that they used the 5-point Likert-type scale to record participant responses to each question in the survey. Of the 988 participants who responded to the online survey, 45% were female while the remaining were male; the mean age was 32. There were 75.6% Caucasians, 7.8% were Asian, 5.8% were African American, and 5.75% were Hispanic.

Tsai et al. confirmed that the study participants were comparable in population to the population of the internet users in the United States.

Tsai et al. (2016) hypothesized among others that the severity of threat will predict security intentions and the susceptibility to threat will also predict security intentions. There was a total of 10 hypotheses, all of which focused on security intentions. In addition to the two hypotheses mentioned above, there were other areas of the PMT that focused on the security intentions. These are coping self-efficacy, response efficacy, subjective norms, safety habit, personal responsibility, and perceived security support. All these components were noted as positively predicting security intentions. Only response cost was noted as negatively predicting security intentions. Tsai et al. tested the hypotheses with a 15-predictor regression model that has 10 predictors and 5 demographic variables. The five PMT predictors were tested through a hierarchical regression analysis.

Tsai et al. (2016) found that security habit strength was the strongest motivator of security intentions, followed closely by response efficacy and personal responsibility. Additionally, coping appraisal variables positively predicted security intentions. A shift that was observed was in the coping self-efficacy variable. Although it significantly predicted security intentions, the relationship was in the opposite direction of what was stated in the hypothesis. The study by Tsai et al. further revealed that the security intentions of internet users were predicted by the severity of online threats and has shed light on the behavior of internet users and how they seek to protect themselves in cyberspace. Governments can also use the results of the study by Tsai et al. to develop

programs that will improve online safety. Online safety, as it relates to the current study, concerns the behavioral intentions of 18- to 21-year-old internet users regarding the protection and security of their personal data in cyberspace. Equally important is the issue of the awareness of the study population concerning cybersecurity. The discussion that follows provides a brief look at the qualitative research methodology and its five underlying approaches.

Qualitative Research Methodology

Qualitative research aims at providing information that is reliable, unbiased, and in a form that the target audience sees as relevant and meaningful (Denzin & Lincoln, 2005; Kruth, 2015). The conduct of most investigations in qualitative research is typically in the natural setting of the participants. The natural setting is where participants are most comfortable and where they can observe the phenomenon in its normal environment (Kruth, 2015). Willig (2013) noted that qualitative research is about meaning and how people experience events as they engage with the world. Kruth (2015) explained how qualitative researchers embrace the concept humans experience regarding events, phenomena, and different situations. Consequently, qualitative researchers are interested in exploring the different human experiences, which will yield invaluable information that aids the extraction of themes and categories (Kruth, p. 2). It is the themes and categories that are the results of painstaking data analysis through effective coding that yields new data in the specific research knowledge area.

Kruth (2015) presented five approaches to qualitative research: phenomenology, narrative, grounded theory, ethnography, and case study. Summarily, narrative research

explores the lives of individuals and events; phenomenology describes the essence of a lived experience; grounded theory refers to the development of a theory grounded in a convergence of data categorization; ethnography refers to studying a culture-sharing group; and case study focuses on developing in-depth description and analysis of a case or multiple cases. The following discussion presents a close look at phenomenology, the chosen approach for this study with its underpinning philosophical understanding and a brief discussion of the other four approaches individually.

Phenomenological Research

Phenomenology refers to the analytic views of the perception of people regarding a definable and specific phenomenon (Dawidowicz, 2016). Patton (2015) posited that phenomenology had its foundation in the philosophical views of the German philosopher Edmund H. Husserl (1913–1954) and the discussions of other philosophers who expanded on his views. One such discussion was based on the work of Alfred Schutz (1899–1959) whose work assisted in establishing phenomenology as a major perspective in social science. Patton asserted that Husserl was the first to apply the philosophical tradition of phenomenology to social science (p. 116). The basic philosophical assumption of Husserl was that human beings can only know what they experience, when they attend to their perceptions and meanings, which awake their awareness consciously (Patton). Moustakas (1994) stated that "the discovery of meanings and essences in knowledge" was the focus of Husserl (p. 38). Broadly, the aim of phenomenology is to gain in-depth understanding of the nature and the meaning of everyday experiences

(Patton). Understanding the meaning of these experiences is the aim of phenomenological studies (Kruth, 2015).

Data collection in phenomenological research studies is primarily through interviews, observation, focus groups, and sometimes documents (Kruth, 2015; Patton, 2015; Willig, 2015). Patton (2015) noted that phenomenological researchers depend exclusively on lengthy interviews with a carefully selected sample of participants who have experienced the phenomenon. The interview could be an exploration of the phenomenon or a philosophical discussion that helps in turning on the lived experiences of the individuals (Patton).

Philosophy of Phenomenology. The philosophy of phenomenology found its roots "in the epoch of Plato, Socrates, and Aristotle as a philosophy of human being" (Fochtman as cited in Qutoshi, 2018, p. 216). Equally, the emergence of the concept of phenomenology can be traced to the philosophical works of Kant, Hegel and Brentano; and it is the writings of these three philosophers, among others, which inspired Husserl (1859–1938) to spend his lifetime in the development of phenomenology [(Dowling; Polit & Beck (as cited in Matua and Van Der Wal (2015)]. According to Habermas (1999), Kant stated that "the transcendental subject determines the conditions of what for it can appear as something in the objective world… and the interaction of the knowing subject and the world is thus again explained in terms of oppositions" (p. 4). Hegel (1994) expanded on Kant's a priori concept by arguing that knowing is made possible through the cognitive tool of phenomenology as noted in the retrospection of Kazeroony (2020) on the development of phenomenology. Brentano's philosophy on descriptive

psychology also influenced Husserl, hence his preference of descriptive over interpretative concerning phenomenology. The philosophy of phenomenology accommodates the use of "open systems of questioning" (Kazeroony, p. 14). The open system of questioning allows contrasting but meaningfully relevant answers to continue to yield contextual structures that are unlimited in the strength of the data being sought by the researcher (Hubick, 2018; Kazeroony).

Philosophically, the primary focus of Husserl's phenomenology was epistemological, which concerns knowledge and how it is acquired (McConnell-Henry et al., 2009). van Manen (2014) noted that Husserl's "epistemological phenomenology remains stuck in a metaphysics of presence and representation" (p. 106). Husserl's assumption was that "transcendental entities and beings" are objects of consciousness (van Manen, 2014, p. 106). However, Heidegger (1962) argued that Husserl (1970) did not explicate what these transcendental entities and beings that are objects of consciousness consist of. All the same, Kazeroony (2020) echoed the beliefs of Husserl (2012) and posited that the essence of the entities and beings that are objects of consciousness, which aids the production of data for epistemological research, emerge with the synthetization of "the eidetic and apodictic generalities of perception" (p. 9). Concerning experiences, Husserl (2012) posited that experiences are containers for natural knowledge that emanates from a person's awareness of *what is*, which develops when intuition connects unconsciousness to the world of human existence. Experiences can only produce knowledge when it connects to other things in the environment (e.g., cultures, locations, settings, and a host of other inclusions within the space of human

existence) (Kazeroony, 2020). Husserl introduced the notion of lifeworld, which means *Lebenswelt* in German, his local language. van Manen (2015) described lifeworld as the everyday life that we live and experience. The idea of lifeworld is the world of lived experiences and how human beings experience it.

Merleau-Ponty (1964) and van Manen (2014) asserted that the conduct of phenomenology must always begin with lived experiences, which occurs prereflectively. Merleau-Ponty challenged Husserl's (1970, 2012) philosophy concerning the description of "the essences of consciousness" and contended that "it is primal lived experiences, wild being, that must be interrogated" (van Manen, p. 131). Merleau-Ponty stressed that interrogation only expresses the primal lived experience, but "can never capture it in descriptions of essences" (p. 131), which is contrary to Husserl's assertion. Merleau-Ponty posited that lived experience should be interrogated through the adoption of "an expressive vocative style in his ontological phenomenology of embodiment" (van Manen, p. 131). Perception of things was a major part of Merleau-Ponty's (1964) philosophical reflections (van Manen). Kazeroony (2020) agreed with Merleau-Ponty and van Manen that phenomenology is entrenched in the inherent constitution of the mind, which facilitates the "primacy of perception to uncover *what is*" (p. 11). Merleau-Ponty posited that the relation of human beings to the world is based on a "relation of perception… that occurs at a primal, corporeal, and preconscious level" (van Manen, p. 128). To Merleau-Ponty, according to van Manen, human beings and the world have an ontological relationship—in which the object affects the subject and vice versa (p. 128). With regards to language, Kazeroony (2020) agreed with Merleau-Ponty that language aids the

understanding of perceptions and that a portion of perception is embedded in language, which is dependent on the comprehensiveness of "phenomenology as the overriding ideation" (p. 11). Phenomenology as the aggregate of all experiential objects supersedes what is perceived and aids the attainment of comprehension globally (Merleau-Ponty; Kazeroony).

Amadeo Giorgi (1997, 2009), a psychologist, is one of Duquesne University's scholars who advanced the scientific psychological phenomenology. Wertz (2010), a student of Giorgi, confirmed the lifetime devotion of Giorgi to the development of descriptive phenomenology as a research method for psychology, human sciences, and other related disciplines. Giorgi drew from the philosophical doctrines of Husserl to develop a purely distinct form of phenomenology, notably the descriptive phenomenological approach (Van Manen, 2014). It is noteworthy that Giorgi derived his impetus from the philosophical writings of Husserl. This is because Husserl was regarded as the fountain of the overall phenomenological movement (Wertz, 2010). All the same, Giorgi still had to add his own empirical scientific twist—a form of personal conceptual uniqueness, to arrive at a purely descriptive analytical form of phenomenology (van Manen, 2014). Husserl is particularly relevant to Giorgi because of Husserl`s reliance on epistemology, the bedrock of the sciences and the inventive research methodology that is usable in studying human experience and psychology (Wertz, 2010). Giorgi's goal was to introduce a logical method that is grounded in the Husserlian phenomenology, but still with a procedural focus that engenders the generation of useful empirical research data. It

is this empirical approach to research that differentiates the descriptive phenomenological principles of Giorgi from Husserl (Aagaard, 2017; Wertz, 2010).

Descriptive Phenomenology. Descriptive phenomenology has its origin from the philosophical works of Husserl (1970, 2012), Merleau-Ponty (1964), and Giorgi (1997, 2009). It was because of the learning acquired from the extensive phenomenological works of Husserl and partly Merleau-Ponty that Giorgi developed his strictly "descriptive approach to phenomenology" (van Manen, 2014, p 210). The focus of descriptive phenomenology is on the purity of its process to obtain "unprejudiced description" from participants concerning the essence of a real world lived experience (Aagaard, 2017, p. 522). Giorgi approved collecting descriptions from other people and procedurally purifying it through bracketing; a way to suspend one's previous knowledge about a phenomenon to remove researchers' biases. This falls in line with Husserl's phenomenological principle of suspending one's prior knowledge about the phenomenon. Giorgi advocated the use of the attitudes that are natural to the people experiencing the phenomenon and phenomenological reduction. In his own words, Giorgi explained that "… the natural attitude is utilized because, practically, one cannot expect all of the persons in the whole world to be phenomenological and thus be capable of assuming the attitude of the reduction" (1997, p. 243). Husserl's philosophical method brings to the forefront the fundamental characteristics of lived experience and the introduction of "reflection on meaning and eidetic analysis using imaginative variation that are required for knowledge and its basic form" (Wertz, 2010, p. 6). It is Giorgi's descriptive

phenomenology that offered the expository procedure, which is available for the descriptive phenomenological study of lived experiences (Wertz, 2010).

Descriptive Phenomenology as a Research method. The process of descriptive phenomenology as a research method begins with a phenomenological interview during which a researcher collects descriptions about a phenomenon from the lived experiences of people who have experienced the phenomenon (Aagaard, 2017; Jackson et al., 2018). Transcription of data follows thereafter to develop the interview transcripts. Next is the extensive repetitive reading of the interview transcripts during which a researcher "suspends or brackets prior knowledge about … the particular phenomenon" to make "sense of the whole" without injecting prior knowledge about the phenomenon (Jackson et al., 2018, p. 3315). The development of meaning units begins. A researcher reads the transcripts again and attaches meaning units to each description of an experience transcribed unto the interview transcript. There is a transformation of the meaning units, by using third-person language, to produce expressions that are pertinent psychologically. The transformation of the meaning units during which a researcher expresses the psychological implications of each meaning units involves an attitude that Giorgi (2009) referred to as the "generic atheoretical psychological attitude" (p. 135). The use of eidetic reduction follows with a researcher "articulating the invariant structure of the given phenomenon" by combining a synthetization of the transformed meaning units that reveals the essence of the phenomenon (Aagaard, 2017, p. 521). A researcher then uses free imaginative variation to determine the essential features of the phenomenon by removing incidentals from its overall description. These processes yield a final general

description of the phenomenon from the collected lived experiences of the people interviewed.

Narrative Research

Kruth (2015) pointed out that narratives are like storytelling. Patton (2015) asserted that the "narrative approach to qualitative inquiry focuses on stories" (p. 128). However, stories and narratives are not the same. Bell (2002) explained that narrative research goes beyond the telling and capturing of stories; story should be treated as the data and narrative treated as everything that is involved in the analysis of the story. Story is what occurred, but narrative is the structuring, interpretation, and the specific scripting of what happened contextually. Narrative research involves the studying of stories about individuals, groups, and significant events by gathering data that are organized and ordered chronologically (Kruth; Patton). The researchers conduct the chronological ordering of the stories and experiences. Participants often may not tell their stories in this order. Czarniawska (2004) defined narrative research as a specific type of qualitative research that is derived from the spoken word or given as a written text that gives account of an event and action or series of both (p. 17). Therefore, stories that provide information on individual identities, experiences, and events for narrative research, as shared in individual and group conversations or documented through written notes, are collected in many ways. It could be through interviews, rhetoric, written text, documentation, journals, diaries, and even observations (Kruth; Patton). Additionally, narrative research participants may talk about many aspects of their lives, which could be

embodied into three phases: the past, the present or the future (Clandinin & Connelly, 2000).

Grounded Theory

Grounded theory was developed through the collaboration of Barney Glaser and Anselm Straus (Glaser & Straus, 1967; Patton, 2015). Glaser and Straus (1967) developed grounded theory using the quantitative research methodology. Patton (2015) explained that both authors later disagreed on the structure and practice of grounded theory and took their ideas in opposite directions. The focus of grounded theory was on grounding a theory from the views of participants using field data collected from the participants (Patton, p. 109). This approach used interviews for data collection with analysis done through coding. The data collection description may erroneously show that grounded theory research method only applies to the qualitative research methodology. However, this is not true. Patton further explained that while grounded theory might be widely seen as an approach that is specific to qualitative inquiry; several other researchers do not see it that way. One such researcher is Glaser (1999) who asserted the generalization of grounded theory as a research approach.

Glaser believed that grounded theory can be used on any research data that is qualitative or quantitative and was developed partially by him using quantitative data; however, this does not limit it to only quantitative research inquiries. Glaser opined that data collection in quantitative research could be more expensive compared to the inexpensiveness of the collection of qualitative data. Besides, Glaser stated that qualitative data are very "rich in meaning and observation, and they are very rewarding to

collect and analyze" (p. 8). Glaser explained that the growing use of grounded theory to conduct qualitative studies has linked it to qualitative data and, as such, is almost always only seen as a qualitative research approach and cautioned that this should not be so. Patton advised that it is prudent for researchers to lean towards qualitative grounded theory when the resources to conduct such research are available, and when it benefits their personal and career rewards.

Ethnography

Patton (2015) posited that ethnography is the main method used in anthropology and is the first well-defined tradition of the qualitative research, and that the idea of culture is at the core of ethnography. It is about a groups' culture and how the culture has shaped their behaviors and perspectives about life (p. 100). Wolcott (2016) explained that ethnography is a form of qualitative research that focuses on the sociological meanings of sociocultural phenomena through the research lenses of commonality. Studying a group that shares the same culture is unique to this approach. In ethnographic research, Fetterman (2010) suggested that researchers look for patterns in the social and cultural behaviors of the people, their ideas and beliefs that are expressed through actions, which are observed by the ethnographic researcher. These discernible patterns, in the social and cultural behavior of the culture-sharing group, are formed over a long period of time as they closely interact with one another. Fetterman confirmed that ethnographic researchers frequently start with a theory that stands as a broad explanation of what they hope to find. Consequently, theory plays an important role in focusing a researcher's attention as they conduct the ethnographic research. Data in ethnographic research are collected through

participants' observation and interviews that may require extensive field work during which a researcher collects symbols, artifacts, and additional diverse sources of data as he/she is immersed in the culture under study. Culture, which is simply defined as *shared knowledge* that people develop as they interact with one another could also occur in organizations and programs (Wolcott, p. 74).

Collection of data has changed with the emergence of the internet. The change has introduced the concept of a virtual ethnographer who studies people who are connected through distributed electronics and networks. Regardless of whichever way data is collected, whether through the virtual space, physical embedment in communities, or nation-states, the distinction that is unique to ethnographic research is that there is always a cultural perspective to the interpretation of data. This interpretation of data affects all types of ethnographic research whether it is applied ethnography that focuses on understanding culture especially when it concerns change efforts of all kinds, or any other type of ethnography research (Patton, 2015).

In addition to the foregoing types of ethnographic research, Patton (2015) also introduced an aspect that is referred to as auto-ethnography, which is the latest and emerging approach to ethnography. Ethnographers have been accused of being biased when they have attempted to study their own cultures, communities, or organizations. This contrasts with the early ethnographic research works that focused on the concept of *other* as ethnographers from Europe travel everywhere to study the people of Africa, Asia, and the Americas, as Patton confirmed. However, things have changed in the new postcolonial and postmodern world that started at the beginning of the 21st century.

The relationship between the observer and the observed has changed. Early observers or researchers are now viewed through the lens of postcolonial sensitivities as being privileged compared to the people of the culture they have studied. Postmodern critiques have raised the question of the influence of the values and the cultural backgrounds of researchers as having affected what they have observed. Add to this the doubt resulting from the question of a researcher's detachment during participants' observation because it was thought that their cultural backgrounds were affecting their observation and the results thereof. Equally important was the question of how ethnographers would study their own culture, which is a shift from going to study other cultures as was the case in the beginning. These developments have contributed immensely to the emergence of autoethnography, which allows ethnographers to study their own culture and themselves as part of that culture while focusing outwardly on the social and cultural aspects of their own personal experiences, and inwardly being able to expose their vulnerable self that may refract and resist objective cultural interpretation (Ellis & Bochner, 2000; Goodall, 2000; Patton, 2015). In autoethnography, researchers use their own experiences to gain insight into the larger culture or subculture of which they are a part. However, what distinguishes autoethnography from ethnography is that the former provides researchers opportunity for self-awareness as they report their "own experiences and introspections as a primary data source" (Patton, 2015, p. 102).

Case Study

Yin (2014) provided a twofold definition that covers the scope and features of a case study inquiry. First, he defined case study as an in-depth empirical study of a case,

or a contemporary phenomenon that is within its real-world context, especially when a clear differentiation between the boundaries of phenomenon and context is difficult to determine. Secondly, Yin described how case study inquiry copes with technically distinctive situations where available data points are not enough to address the various applicable variables. A vivid example could be studying resilience or excellence as a theoretical concept, or the study of a disease that a patient is suffering from, or it could be specific like the case study of a military operation as documented in Engberg (2013). Regardless of the differences among cases, Patton suggested that placing an arbitrary boundary around the cases of interest is what is common to all cases. The boundary determines what the case is and the focus of the study.

Leedy and Ormrod (2015) indicated that a case study focuses on the in-depth studying of an individual, event, or program for a specific period, and added that some researchers see a case as an object of study while others see it as a methodology. Yin (2014) contended that data collection in case study research relies on multiple sources of information or evidence. Pulling data from multiple sources for necessary data convergence aids the attainment of data triangulation. Yin added that a case study research benefits from available theories and these guide the collection and the analysis of data (p. 17).

Yin (2014) determined that case study research is not limited to only qualitative research, but also extends to quantitative research, and argued that the use of a mixture of both qualitative and quantitative evidence to define a case or cases is what proves that case study is not only a qualitative research methodology, but also leads to the inclusion

of mixed-method research methodology in conducting case study research. Additionally, most researchers tend to lean to the use of single case due to its specificity and uniqueness, which aid understanding and ease of use. Others combine two or more cases for the purpose of comparisons and build theory or propose generalizations (Leedy & Ormrod, 2015). The discussion that follows provides a brief look at cyberspace, cybersecurity, its definition, the space in which it occurs, and the concepts of personal data protection and cybersecurity awareness.

Cyberspace

The interaction among internet users takes place in cyberspace through information systems. Cyberspace is a virtual platform of interconnected computer networks that are linked through cables and routers, which allow for communication, storage, and retrieval of information. Singer and Friedman (2014) described cyberspace as an information environment through which information moves between computer and computer clusters, where humans are the generators and users of the information. The introduction of human weaknesses through behavioral intentions while interacting in cyberspace could hurt users and expose information systems to unnecessary vulnerabilities. The users of information systems are often identified as the weakest link in information security (Bulgurcu et al., 2010; Warkentin & Willison, 2009). Crossler et al. (2013) confirmed that individual users remain an area of weakness that are often overlooked.

Toward a Unified Definition of Cybersecurity

Craigen et al. (2014) conducted a qualitative study to develop a new definition for cybersecurity and explained that there were various interlocking discussions in the field of cybersecurity, but there appeared to be no widely accepted concept towards a new definition that will closely align with the interdisciplinary nature of cybersecurity. Craigen et al. (2014) conducted an in-depth literature review of relevant literature that covered journals from a wide scope of sources from the academic disciplines, mostly from computer science, engineering, technology, security, and defense. Other literature included, to a lesser extent, were literature in political studies, management, education, law, and other disciplines that they did not mention. In Craigen et al.'s review process, they identified five dominant themes and distinguishing aspects of cybersecurity. As a result of the QDA of the selected articles, Craigen et al. selected nine definitions of cybersecurity from the identified dominant themes and distinguishing aspects, which were then presented to a multidisciplinary group of authors and graduate students of technology for discussion to get their critical context to the cybersecurity definition process.

Craigen et al. (2014) did not provide a detailed explanation on the reason these individuals were selected as members of the multidisciplinary group other than they were experienced cybersecurity professionals and technological graduate students. The only qualitative research explanation that could be ascribed to the selection of these members was that the researchers used purposeful sampling to select them based on their knowledge and experience in cybersecurity.

According to Patton (2015), purposeful sampling is defined as the sampling strategy primarily used in qualitative research. The sampling strategy allows a researcher to deliberately select individuals and sites for the research study because they have information that would be of benefit to the study. Patton defined purposeful sampling as a technique that is widely used in qualitative research for the identification and selection of information-rich cases for the most effective use of limited resources. Patton explained that information-rich cases are those cases or individuals a researcher can learn from concerning the "issues of central importance to the purpose of the enquiry" (p. 230). Patton further explained that in-depth understanding about the purpose of a qualitative enquiry comes from information-rich cases and asserted that purposeful sampling is better than the empirical generalization that comes from random sampling prevalent in quantitative research methodology.

Comparatively, Patton (2015) discussed the logic between random and purposeful sampling and believed that the power of random sampling comes from representativeness where samples are drawn randomly from a population, and that it is based on the statistical probability theory. Patton asserted that random sampling provides the confidence to generalize from a sample to a larger population. This is the very purpose of random sampling—it guides against selection bias that could be present in purposeful sampling. What is looked at as bias and weakness in statistical sampling is seen as an opportunity for deliberate focus in qualitative sampling and, as a result, is seen as strength. This is the reason purposeful sampling targets cases that are rich in information and are sought by a researcher in a research study.

At the end of the study, Craigen et al. (2014) proposed a new definition for cybersecurity that was all inclusive. The new definition of cybersecurity proposed was "the organization and collection of resources, processes, and structures used to protect cyberspace and cyber-enabled systems from occurrences that misalign de jure from de facto property rights" (Craigen et al., p. 17). A discussion on cybersecurity awareness through the lens of qualitative research inquiries now follows.

Cybersecurity Awareness

Rahim et al. (2015) and Siponen (2000) described cybersecurity awareness as a methodology to provide necessary education to internet users so that they could be sensitive to the various cyberthreats and the vulnerability of computers and data to these threats. Chanderman and Van Niekerk (2017) also provided a description of cybersecurity awareness. Before providing a description of cybersecurity awareness, Chanderman and Van Niekerk shared Van Solms and Van Niekerk's (2013) definition of cybersecurity, which refers to the security and protection of cyberspace with the interplay of all the real and virtual technologies that operationalize it. It is the users whose behaviors, in its diverse existential capacities, determine the various dynamics in cyberspace. Based on this paraphrased definition, Chanderman and Van Niekerk provided their description of cybersecurity awareness: comprises the knowledge and skills that are actual and self-perceived attitudes and behavior, and the relationship that exists among these elements (p. 134). Cybersecurity awareness is also defined as the extent to which users understand the importance of information security, and the

responsibility of users to protect the organizations data and networks by exercising appropriate levels of information controls (Rahim et al., 2015; Shaw et al., 2009).

Rahim et al. (2015) explained that cybersecurity awareness was meant to alert internet users of cybersecurity issues and threats and enhance internet users' understanding of the dangers concerning cyberthreats so that they could embrace security any time they are using the internet. Cybersecurity awareness should not represent a source of fear or apprehension. Rather, it should be used to educate users so that they are armed with contingency plans that would act as deterrence to cyber-attacks. Additionally, cybersecurity awareness provides an invaluable platform for the dissemination of information regarding new cyberthreats since threats in the cyberspace continues to evolve as cybercriminals look for novel ways to carry out their nefarious acts.

Importance of Cybersecurity Awareness

Cybersecurity awareness in recent years has become important due to changes in cyberthreats because of the increase in the global population of internet users. The population surge seems to have been caused by the additions of new applications like those for online banking and shopping, virtual broadcasting, and the virtual interactive sharing of information through social media (Rahim et al., 2015). Internet users vary and the group of users that are often reported as mostly vulnerable in cyberspace are those between the age of 12 and 19 (Rahim et al., 2015). The reason was that adolescents, when compared to other communities of internet users, are highly active with online shopping, and spend more time in their use of online media content. Equally, this age group values social networking sites more and see it as an invaluable way to maintain their

relationships (Cole et al., 2013). These interactions on the Web are carried out using internet applications, which open adolescents to various forms of cyberthreats. Consequently, the online behavior of young people comes with associated problems that allow cybercriminals to exploit the applications they interact with on the Web and to launch diverse forms of online attacks against them (Atkinson et al., 2009). These attacks could be in the form of secret invasion or outright stealing of an individual's private information that culminates into identity theft. Additionally, the cyberthreat landscape has shifted from the narrowly targeted cyber-attacks on a group of internet users to the use of sophisticated and well-planned strategies.

Chanderman and Van Niekerk (2017) posited that the names and social security numbers of approximately 280,000 AT&T U.S.-based customers were stolen by AT&T datacenter workers in the Philippines and sold to interested third parties. As a result of this incident, the Federal Communications Commission fined AT&T $25M for failing to protect the personal data of its customers (Ruiz, 2015). The shift in the sophistication of cyber-attacks has made cybersecurity awareness, through which a counter-measure strategy could be put in place, essential for internet users such as the population of this study. The counter-measure strategy, through cybersecurity awareness, would assist in combating silent privacy invasion concerning the population of this study (Choo, 2011; Dlamini et al., 2009; Furnell et al., 2008). The well-planned counter-measure strategies would ensure an appropriate platform through which security culture could be instilled in adolescents for their personal data protection and other internet users alike. Consequently, it is critical for the messaging of cybersecurity awareness education to be

effective so that it can provide a general understanding of cybersecurity understanding across all ages including the adolescents and cybersecurity managers who are the focus of this qualitative phenomenological study. Equally, it is critical to ensure that the message of cybersecurity awareness programs is well-conveyed so that it could be well received by adolescents and other internet users in cyberspace (Rahim et al., 2015). The message disseminated through a cybersecurity program must be accurate, concise, and clear in its presentation so that it can be easily understood. The message must be planned and deliberately targeted at a specific audience, as would be the case with the population of this proposed study.

Rahim et al. (2015) stated that "many researchers have called for urgent measures to introduce cybersecurity awareness, because it is one of the top requirements of the Internet community today" (p. 607). However, this call for urgent measures comes with some challenges, especially where the adolescents are concerned. A few of these challenges are discussed below.

The first challenge was finding a way through which adolescents would understand and accept appropriately the cybersecurity concept and then promoting the advancement of a security culture among adolescents (Kruger & Kearney, 2006). The second challenge is determining the type of message that should be conveyed to adolescents in a cybersecurity awareness program to avoid the one-size-fits-all messaging, which will not benefit them. The third challenge concerned the overall effectiveness of the ways to educate adolescents about how they should address threats,

especially identify theft (Loibl, 2005). Therefore, to mitigate the adverse effect of these challenges, there is a need for future cybersecurity awareness studies.

Qualitative Analysis of Cybersecurity Awareness

Rahim et al. (2015) conducted a systematic literature review (SLR) to assess the approaches to cybersecurity awareness and followed a streamlined step-by-step approach after conducting an extensive SLR of peer-reviewed articles with empirical studies. Rahim et al. explained their inclusion and exclusion criteria and confirmed the use of Google Scholar, Science Direct, the Institute of Electrical and Electronics Engineers (IEEE), the Emerald, and Springer databases. Excluded publications were editorials, informal articles from organizations, book reviews, article summaries, interviews, news, and trade journals, because only full-text and peer-reviewed articles were needed for the study. In the SLR of the selected articles, Rahim et al. chose the Kirkpatrick's four-level learning model of evaluation that was recommended by Abawajy (2008) and Karjalainen and Siponen (2011). Based on these recommendations, Rahim et al. used a systematic program evaluation technique for the assessment of cybersecurity awareness. The four-level Kirkpatrick's learning model, which supported quantitative and qualitative methodologies, was based on the evaluation theory derived from the benefit of the program theory and the social science theory. Summarily, the program theory "is founded on the logic connection between a program's input and output, while the social science theory promotes the concept of human development, learning, and changing behavior" (Rahim et al., p. 601). The Kirkpatrick's four-level learning model was then used to investigate the four levels: reaction, learning, behavior, and results. Rahim et al.

explained that cybersecurity awareness research would require a combination of methodologies because the assessment of human beings should not be based on only one approach (p. 615). Consequently, they conducted this qualitative phenomenological study with a little injection of the mixed-method research inquiry. In addition to using the Kirkpatrick's four level learning model, Rahim et al. also used matrix analysis to answer each research question and provided matrix analysis of assessment methodologies, the target audience, and the scopes of assessment that was identified in the study. The researchers posited that matrix analysis consisted of horizontal lines that show a list of what was to be assessed.

Rahim et al. (2015) predicted that the outcome of their assessment will help to facilitate the capability of the cybersecurity awareness program modules in providing cybersecurity education. This was found to be true. Additionally, they found that no previous cybersecurity awareness assessment had used the program evaluation technique to assess user awareness. Equally, Rahim et al. found that though "good methodologies have been used to study cybersecurity awareness, there was still a lack of flexibility with using multiple methodologies in one study" (p. 618). The researchers concluded that when users or audiences are categorized, it ensures that the right cybersecurity message is delivered to the appropriate group. The researchers explained that the adolescents, who were between the ages of 12 and 19, were not categorized in the study, hence they recommended future research where they can be categorized either as one unit or partially as needed for further studies. The current study uses the qualitative research methodology and not the mixed-method research methodology. The use of a mixed-

method research methodology to study these groups would be an opportunity for future research concerning this population.

Personal Data Protection

Kritzinger (2017) noted that the personal information of school learners has been put at risk as the learners use different kinds of ICTs. Because cybersecurity awareness is essential to most school learners, understanding the knowledge of school learners in cyberspace is important. Equally essential, is the knowledge of the school learners concerning cyber-safety. Kritzinger suggested that the lack of understanding of cyber-safety by school learners could lead to the reckless sharing of personal data, which cybercriminals could exploit in cyberspace.

Kritzinger (2017) used closed and open-ended questions in a quantitative study to survey 503 high school students between the ages of 16 and 19 who used the internet. The gender split of study participants was 55% male and 45% female. The racial split was 44% Black, 25% White, and 31% were classified as *Other*. The online activities of this population ranged from social networking, surfing the internet, playing online games, and visiting chat rooms. The survey was Web-based and contained 47 questions. Of the 47 questions, 8 were open-ended and 39 were closed. Kritzinger conducted the study primarily to determine the school learners' current state in cyber-safety awareness. An additional focus of the study was the identification of role players who must aid cyber-safety awareness and education.

Kritzinger (2017) did not share how he conducted data analysis but provided the result from the analysis of the responses from participants and found that majority of the

study population had not paid adequate attention to upholding cyber-safety culture while they interacted in cyberspace. Participants who were 63% of the study population responded that they had watched inappropriate content online; 57% confirmed that they had shared personal information on an online site; 72% confirmed that they had used their real name and other PII on an online website; and 33% confirmed that they had shared their telephone numbers with someone online that they did not know. The study also revealed lack of parental control—64% indicated that there is no parental control concerning their online activities; 86% responded that they did not need permission from their parents to engage in online activities; and 82% responded that they have access to the internet from their bedrooms and can surf the Web anytime.

Kritzinger (2017) used these findings, in addition to other findings in the study, to develop a cyber culture approach that will aid in the cultivation of cyber-safety while interacting in cyberspace. Listed in the approach are the roles of all stakeholders involved in ensuring a cyber-safety culture. Government should develop cyber-safety guidelines and strategies aimed at protecting learners who are the study population. Parents and teachers should receive continuous training and support and schools should develop or adopt cyber-safety guidelines and policies aimed at ensuring the safety of school learners.

Öğütçü et al. (2016) analyzed personal information security risky behavior and found that users' undesirable behaviors are closely related to users' information security awareness. Öğütçü et al. investigated the preventive actions employed by internet users due to threat exposure and the effect it has on them, and their study showed that information systems users are the biggest threat to information security as they represent

the weak spot in an information security defensive armor. This is in line with Abawajy's (2014) findings that, regardless of the strength and different layers of information security defenses, the security of information systems is still dependent on the behavior of users. Abawajy noted that information technology components are contemporarily more secured, and cybercriminals have shifted their focus from components to attacking unsuspecting users who represent the softest links in an information systems networking infrastructure. Abawajy further noted that the only way to reduce the penetration of cyberattacks is to focus on the human behavior of users who are often exploited by cybercriminals.

Sithira and Nguwi (2014) cautioned that adolescents' online behavior and their excessive use of the internet have opened them up to cyberspace vulnerabilities like identity theft and other online fraud. The purpose of this qualitative phenomenological study is to provide research data on the current online security knowledge and skills of the youth population. Sithira and Nguwi further cautioned that youth and teenagers face online danger as they experiment with social media. Compounding this problem is the large amount of time they spend online, which culminates into excessive use of the internet with little knowledge for self-regulation. Sithira and Nguwi provided data on the ownership and usage of cell phones, which revealed that "out of 75% of teenagers owning cell phones, 25% use them for social media, 24% use them for instant messaging, and 54% use them for texting" (p. 1). The knowledge of this teenage population, concerning the online protection of their data when they interact on the internet, is not well known.

Sithira and Nguwi (2014) used closed and open-ended questions to investigate the common online activities of the study population and their behavioral intentions towards such activities. Closed and open-ended questions were used in a survey that included 13–15 questions. The purpose of adding open-ended questions to the questionnaire was to collect in-depth narrative response from study participants. Sithira and Nguwi erroneously did not provide the age and the number of participants for the study who were adolescent males and females.

Sithira and Nguwi (2014) found that many of their study participants admitted to sharing their personal information online. Responses from participants confirmed that the sharing of personal information is the riskiest activity online. The study revealed that female students, in comparison to male students, were "bolder and more vocal" online (p. 6). Sithira and Nguwi recommended guidance and online security education for this population of internet users to ensure they are equipped with adequate security awareness that will protect them while interacting on the internet.

Magolis and Briggs (2016) studied the social networking site (SNS) knowledge of the undergraduate seniors who are in the age range of 20 to 22 years. The purpose was to examine the lived experiences of this population regarding the type of information they share on social networking sites. Magolis and Briggs noted an increase in the invasion of privacy of the study population, due to the increased messaging in "audio, video, and multimedia" (p. 22) on SNS sites. Magolis and Briggs posited that there is controversy concerning young adult privacy on SNS sites. Most of the population is protected in high school due to the protective restrictions by most school districts; 70% of the school

districts do not allow the population to access SNS. However, the protection is removed when the population gets into college, hence the need to study the online privacy awareness of the population on SNS sites.

Magolis and Briggs (2016) conducted a qualitative phenomenological study to explore and understand the populations' experiences concerning SNS data privacy. Magolis and Briggs conducted face-to-face interviews with eight undergraduate seniors, who were students at a university in the northeastern United States. The composition of participants for the study was four males and four females. The researchers interviewed each participant twice during the semester. The interviews that occurred at the beginning and the end of the semester lasted for 60 minutes and 30 minutes, respectively. The questions for the interview were open-ended and facilitated the collection of in-depth rich data that represented the lived experiences of the study participants.

Magolis and Briggs (2016) followed the qualitative phenomenological approach in the analysis of the interview data, and read the interview scripts, field notes, and memos twice, then developed brief memos. A third read-through of the interview transcripts led to the development of line-by-line coding, which aided in the development of nine meaning units that the researchers discussed and analyzed in four separate periods. The researchers developed general themes from the nine meaning units based on similarities. Additional analyses of interview transcripts and field memos continued till the researchers reached a point of saturation when no additional themes were discovered.

Magolis and Briggs (2016) found from the analysis of data that majority of the study population openly shared their personal data on SNSs. This finding came out of the

first theme, which was “openly shared personal information” (p. 27). Five out of eight participants who represented 71.4% admitted to sharing their data on a SNS. Personal information in this qualitative phenomenological study refers to “a person’s interest, likes, dislikes, opinions, and other non-demographic data” (pp. 27–28). These five participants were aware of the visibility of their personal data to others online and they were pleased about it. A subtheme to theme one was “Don’t cross the line: Limits on personal location” (p. 28). There was a common theme among participants’ analysis of data that showed they were unwilling to share details on their physical location on SNSs. Participants considered being located by anyone online as an online privacy violation.

Theme two from the data analysis was “I want to be seen” (p. 29). Four participants were willing to share their background information on SNSs. Background information refers to demographic data like age, hometown, sex, and other demographic data. These participants felt sharing their demographic data was important because it would allow friends and nonfriends to connect with them online. A subtheme to the second theme was “Choosing what to share could lead to employment” (p. 29). The four participants who were willing to share their demographic data believed that it would help potential employers contact them. Other study participants were cautious about sharing demographic information on SNSs.

A third theme was “Personalized Privacy Settings” (p. 30). Magolis and Briggs (2016) explained that participants were divided in the choice of their privacy settings but did not provide specific data on the participants’ split. Magolis and Briggs further explained that participants belong to two factions: private profiles and public profiles.

Participants with private profiles used the privacy settings on SNSs in addition to controlling what they shared online. A common theme between both factions was that they felt they had control over what they shared online depending on their information exposure tolerance. The findings in this qualitative phenomenological study revealed that the study participants were aware of their online privacy, and they have control over personal and background data they should share online.

Summary and Conclusions

Chapter 2 included an introduction that presented a restatement of the specific management problem and the purpose of the research study which was to explore the lived experiences of cybersecurity managers in the metro areas of Washington D.C., Maryland, and northern Virginia who have adopted new security laws, new applications, and the IoT to protect users' privacy. The literature review strategy presented a listing of the search engines and the keywords used in numerous online searches for peer-reviewed articles, and other sources of information for the research study. The concepts of personal data protection and cybersecurity awareness, which are central to the focus of the study, were fully discussed under conceptual framework. Equally discussed, is the behavioral intentions of the study population through an aspect of the PMT. Discussion also focused on qualitative methodology, which is the preferred methodology for the research study. The five major approaches to qualitative research—narrative, phenomenology, grounded theory, ethnography, and case study—were part of the discussion. There was justification for the choice of phenomenology as the preferred approach for the research study. Further discussion focused on cyberspace, cybersecurity, cybersecurity awareness, personal data

protection, and identity theft. Literature reviews of relevant peer-reviewed articles were embedded during the discussion of the keywords. This summary and the transition statement that follows end the chapter. Chapter 3 contains the research method.

Chapter 3: Research Method

Introduction

The purpose of this descriptive phenomenological study was to explore the lived experiences of cybersecurity managers adopting new security laws, new applications, and the IoT to protect users' privacy in the metro areas of Washington, D.C., Maryland, and northern Virginia. Data were collected through interviews with a purposefully selected sample of the study population using an interview protocol with open-ended questions**.** The study may provide an opportunity to learn about the lived experiences of cybersecurity managers adopting new security laws, new applications, and the IoT to protect users' privacy.

An interview protocol containing 10 open-ended questions guided data collection through in-depth interviews. The interviews and instrument aided the exploration of the lived experiences of cybersecurity managers in their adoption of new security laws, new applications, and the IoT to protect users' privacy in the United States (Boyce & Neale, 2006; Brinkmann & Kvale, 2015; Myers & Newman, 2007; Oltmann, 2016; Patton, 2015). The findings of this descriptive phenomenological study may provide actionable data concerning the practice of cybersecurity, personal data protection, and privacy concerning the study population.

Chapter 3 includes the purpose of the study, research design and rationale, and an explanation of the role of the researcher. The discussion on my role as the researcher covers ethical issues and biases and how to manage them and justification for the use of incentives. Chapter 3 includes a discussion on the participants' selection logic, the study

population, and the sampling strategy. The discussion also includes data collection methods and techniques, data instruments, and data analysis. Further discussion focuses on the issues of trustworthiness that include credibility, transferability, dependability, and confirmability. Chapter 3 ends with a discussion on ethical procedures, including the Walden University Institutional Review Board (IRB). A summary that presents the main points of the chapter and a transition statement to Chapter 4 ends Chapter 3.

Research Design and Rationale

The overarching research question that guided this descriptive phenomenological study is *What are the lived experiences of cybersecurity managers adopting new security laws, new applications, and the IoT to protect users' privacy in the United States*? The concepts of data protection motivation and cybersecurity awareness are central to the focus of this descriptive phenomenological study. Zadvinskis et al. (2018) confirmed the use of qualitative phenomenological research to explore issues and concerns in depth and detail. Zadvinskis et al.'s confirmation aligns with the purpose of this descriptive phenomenological study, which was to explore data on the lived experiences of cybersecurity managers on their adoption of new security laws, new applications, and the IoT to protect the privacy of individuals in the United States. The chosen methodology for this study was the qualitative research methodology, which provides the opportunity to ask open-ended questions from study participants (Patton, 2015). In contrast, the quantitative research methodology would not have allowed the use of open-ended questions, which is why it was not the preferred research method for this descriptive

phenomenological study. Galt et al. (2019) and Covell et al. (2012) confirmed the use of closed-ended questions in quantitative research.

Role of the Researcher

The role of the researcher in this descriptive phenomenological study was to interview and observe participants, collect data, conduct data analyses, and present and discuss the findings of the study. The participants in the study were cybersecurity managers. My plan was to conduct semistructured interviews with 16–20 participants among cybersecurity managers in the United States metro areas of Washington, D.C., Maryland, and northern Virginia. I guided against biases by ensuring I had no personal and professional relationship with any of the participants. I applied caution to guide against any form of bias and participant prejudice. Equally, I avoided the use of structural sentence constructions that may imply bias against participants in terms of their gender, sexual orientation, age, and ethnic grouping (American Psychological Association, 2009). Participants were selected from outside my work environment to avoid any conflict of interest. I protected the anonymity of research participants and developed trust with each of them (Patton, 2015). Protecting participants' anonymity promotes the integrity of the research study and aided in the collection of unrestricted data from study participants.

Methodology

I conducted a descriptive phenomenological study. In this section, I discuss the methodology for the research study, including participant selection logic, study population, sampling strategy, and the number and rationale for the number of participants. I will include how participants were identified, contacted and recruited. I

will discuss the data collection instrument, the actual collection of data, and the data analysis plan.

Participant Selection Logic

The population for this research study was cybersecurity managers in the metro areas of Washington, D.C., Maryland, and northern Virginia. This population of internet users manage cybersecurity as individual users; their lived experiences in the adoption of new security laws, applications, and the IoT, managing the privacy of individuals is critical. Shillair et al. (2015) asserted that individual users are the key factor in information and cybersecurity. Users of information systems are often identified as the weakest link in information security (Bulgurcu et al., 2010; Warkentin & Willison, 2009). Therefore, ascertaining the knowledge of this population in cybersecurity, personal data protection, and privacy was essential. An effective sampling of this population was necessary to ensure a representative sample for the study.

The purposeful sampling strategy that aligns with the qualitative research methodology is the preferred sampling strategy for this descriptive phenomenological study. Purposeful sampling allows for the deliberate selection of appropriate participants for a research study. I used this sampling strategy to select information-rich participants who were cybersecurity managers who have experienced the phenomenon under study. The phenomenon in this research study was the protection of users' privacy through the adoption of new security laws, applications, and the IoT by cybersecurity managers. Participants were cybersecurity managers who have 5 or more years of information and cybersecurity experience.

In addition to using the purposeful sampling strategy to select a pool of study participants in the metro areas of Washington, D.C., Maryland, and northern Virginia, I also used purposeful random sampling to select the final sample for the study. The planned sample size for my research study was between 16 and 20 participants, depending on when data saturation was reached. I recruited participants through the purposeful identification of information-rich participants who were cybersecurity managers. I posted an IRB-approved recruitment script to a Facebook group hosted by an educational services company that helps professors navigate online education. I also recruited participants through LinkedIn, Project Management Institute, and the Walden University research participant database.

Once participants indicated interest in participating, I sent an IRB approved script to each potential participant. The script included a summary of the purpose of the study, the sampling requirement, and verification information to check that the potential participants met the requirements. If prospective participants met the requirements, a letter of invitation to participate was sent. When participants agreed to participate, I sent an informed consent form via email, which was accompanied by an attachment of a sample of the interview questions. Other information included in the informed consent was assurance of anonymity and an explanation concerning the audio recording of interviews.

For this research study, I planned to conduct 16 interviews; however, final interviews planned could have been below or above 16 participants, depending on when data saturation occurred. According to Fusch and Ness (2015), “data saturation is reached

when there is enough information to replicate the study; when the ability to obtain additional new information has been attained, and when further coding is no longer feasible" (p. 1408).

In the absence of data saturation, I had two options available for consideration (Twisdale, 2018). One option was to continue interviewing more participants until data saturation occurred. The second option was not to conduct additional interviews if doing so would have been time consuming and costly. Twisdale (2018) suggested ending a study with the findings available might be appropriate. The lack of saturation would create an opportunity for further studies when time constraint and cost are no longer an issue. Nonetheless, my goal was to ensure that data saturation was reached.

Instrumentation

Data were collected through interviews conducted via telephone and Zoom video calls. Face-to-face interviews were not possible due to current restrictions because of the COVID-19 pandemic. According to Myers and Newman (2007), there are three different types of interviews in qualitative studies: structured, group, and unstructured or semistructured interview. Structured interviews require the preparation of complete interview scripts, which are often sent to participants or used in surveys (Myers & Newman, 2007). Improvisations through follow-up questions are usually not possible in structured interviews because a researcher does not directly conduct the interview. Group interviews allow a researcher to interview two or more people at the same time (Myers & Newman, 2007). I did not use this interview type because of the potential risk of violating the privacy of participants. In addition, a group interview could have led to the distortion

of experiences described by participants when they listen to each other. Unstructured or semistructured interviews allow the use of an incomplete script with questions prepared beforehand by a researcher (Myers & Newman, 2007). This allows necessary improvisation and the injection of follow-up questions based on the responses from the study participant as the interview progresses (Myers & Newman, 2007; Twisdale, 2018). A semistructured interview is frequently the choice of qualitative researchers who conduct information systems research studies (Myers & Newman, 2007). Consequently, I selected unstructured or semistructured interviews for this research study.

I used telephone and Zoom video calls to interview participants. Telephone interviews and Zoom video interviews compare well with face-to-face interviews (Oltmann, 2016). Oltmann (2016) posited that telephone interviewing has become increasingly common in qualitative research. Holt (2010), Opdenakker (2006) and Vogl (2013) have experimented with telephone interviews and concluded they compare favorably with face-to-face interviews. The advantages of using telephone interviews are reduce costs, access to geographically dispersed study participants, increased safety for the interviewer, ability to take notes unobtrusively, and ease of interview scheduling (Novick, 2008; Oltmann, 2016). Other advantages include the enhancement of anonymity and privacy and an increase in number of potential participants agreeing to participate in the study.

An interview guide with open-ended questions was the collection instrument that guided all data collection activities. I developed the interview guide for the research study using the sample interview guide in Boyce and Neale (2006). Boyce and Neale suggested

that interview guides should include an introduction that contains informed consent, interview questions, and closing comments. The closing comments include information about what comes next after the interview and a statement of appreciation for the participants' time. The central research question guided the development of the interview questions in this study. Keywords from the central research question and the conceptual framework guided the development of interview questions in the interview guide. I followed the recommendations of Jacob and Furgerson (2012) to develop open-ended interview questions. Basic questions focused on respondents' background information were the first set of questions. Beginning the interview with basic questions helps ease respondents into the interviewing process (Jacob & Furgerson, 2012).

Procedures for Recruitment, Participation, and Data Collection

Recruitment of participants followed IRB procedures. No recruitment of participants began until I received IRB approval. The population for this research study was cybersecurity managers in the metro areas of Washington, D.C., Maryland, and northern Virginia. I planned to conduct telephone and Zoom video call interviews with 16 participants. Data collection was planned to occur over 4 weeks, with a possible extension if necessary to accommodate participants' time requirements. The duration of each participant interview was 30–60 minutes.

An approved interview protocol with open-ended questions guided the data collection process. During interviews, a researcher should (a) be conversational, (b) begin the interview by introducing themselves and the study, (c) provide the reason for conducting the study, (d) explain why the research is of interest to the study population,

(e) inform participants of the length of the interview, (f) assure anonymity, (g) request participants' permission to record the audio of the interview, and (h) remind participant they can decline any question they do not wish to answer (Brinkmann & Kvale, 2015). All these steps guide the conduct of interviews during data collection in the field.

At the completion of interviews and data analysis, interested participants received completed interview transcripts for the opportunity to provide feedback. The feedback facilitated the validation and correction of collected data. Afterward, I engaged in quick conversations with participants to clarify key points and answer questions. Finally, I sent thank-you notes with incentives to all participants, thanking them for their participation in the study.

Data Analysis Plan

The data analysis plan includes a restatement of the purpose of the research study, the central research question, and an explanation of the relevance and application of the conceptual framework. Patton (2015) asserted that the purpose of the inquiry drives the analysis and explained the need for researchers to reengage with the research question and the purposeful sampling strategy, which has guided the study design for needed clarity on how to proceed. Patton provided some tips for QDA and asserted that analysis should begin during data collection on the field. Consequently, recording of patterns and themes that emerge from participants' responses would begin on the field while data collection is taking place. The patterns and themes will relate to the central research question, and these would be driven by perspectives from the study participants. All interview questions would follow the keywords and decomposition of the keywords from

the research question and the theoretical framework. The overarching research question that reflects the purpose of this descriptive phenomenological study is: *What are the lived experiences of cybersecurity managers adopting new security laws, new applications, and the IoT to protect users' privacy in the United States?* The protection of individual privacy, personal data protection, and cybersecurity awareness that are central to the focus of this study will guide data analysis. Also important is the decomposition of keywords into related sub keywords. A few of the sub keywords are security laws, applications, IoT, cybersecurity, identity theft, identifiable information, internet information-sharing, and usage. These sub keywords and other emerging themes from the field during data collection will also guide data analysis.

Rubin and Rubin (2012) recommended seven steps for the analysis of data. Two of these are transcription and summarization of the interview transcript. After the completion of data collection on the field, a quick read-through of interview transcripts will follow. The read-through will reinforce my understanding of the responses of the interviewees and aid the quick transcription and summarization of the interview transcripts. After this, I will develop nodes in NVivo, import transcribed data into the nodes, and generate codes that will represent the data and the overarching research question. The codes generated will aid identification of patterns, relationships, and themes. Categorization of codes into themes that are in alignment with the research question will follow. Finally, the coding process will continue to answer the research question until no new codes and themes are found. Rubin and Rubin recommended the storing of relevant concepts, themes, and related information in a single data file. I plan to

accomplish this through the coding process, by first developing nodes that will act as the converged points for the organization and storage of appropriate data.

Saldaña (2016) believed that the coding of data is essential to the research process, and data analysis should begin with the coding of data and recommended first and second coding cycles. The type of research questions on which interview questions are based, also inform the choice of coding method(s) within these two cycles. The central research question for this descriptive phenomenological study is exploratory and focuses on understanding the lived experiences of the study participants, concerning the protection and security of their personal data and individual privacy in cyberspace. Saldaña stated that the coding methods, which would better catalogue and reveal the salience of the study central research question are the "In Vivo, Process, Emotion, Values, Dramaturgical, Focused Coding, and Theming the Data" (p. 70).

Of these coding methods, focused coding is preferred for the initial analytic and strategic coding, which will begin through the formulation of codes from the interview questions. Saldaña encouraged qualitative researchers to "develop your own coding methods … and data analytic processes" (p. 74). Another practical recommendation I plan to use is from Ms. Jessica Dempsey, the Walden University NVivo Support point of contact.

Based on these two recommendations, I plan to begin coding by using the keywords from each of the interview questions. The number of interview questions with their keywords may determine the number of codes for the data analysis. There will be categorization of the codes to ease the data analysis process. The categories will facilitate

organization of data as I read the interview transcripts and search for themes. Themes, which are words and expressions of the same idea and concept, will be assigned to appropriate categories.

I plan to use NVivo, a computer assisted Qualitative Data Analysis (QDA) software for data analysis. Before the final decision to use NVivo, a comparison of NVivo with other QDA software will occur. In the comparative analysis, I will look at five QDA software, including NVivo from the Boston University qualitative software comparison presentation (Boston University, n.d.). The QDAs are: NVivo, Atlas.ti, HyperResearch, Dedoose, and Coding Analysis Toolkit (CAT). The discussion that follows presents the issues of trustworthiness for this research study.

Issues of Trustworthiness

Lincoln and Guba (1985) defined trustworthiness in qualitative research as the extent to which people have confidence in the findings of a qualitative study. Focusing on qualitative inquirers, Polit and Beck (2012) defined trustworthiness as the extent to which qualitative researchers have confidence in their research data. So, to ensure trustworthiness and rigor in the findings of qualitative research, qualitative researchers must address four criteria: credibility, transferability, dependability, and confirmability (Anney, 2014; Salvador, 2016; Schwandt, Lincoln, & Guba, 2007; Shenton, 2004). The next few pages present a brief discussion of the four criteria of research trustworthiness.

Credibility

Credibility refers to the truth and the confidence inherent in the data collected from research participants, and the researchers' transcription and representation of it

(Cope, 2014; Patton, 2015). Patton (2015) stated that credibility addresses the "issue of the inquirer providing assurances of the fit between respondents' views … and the inquirer's reconstruction and representation of same" (p. 685). Cope acknowledged that credibility strategies, among others, include triangulation, member checking, peer review, and reflexivity (field journal). Carter et al. (2014) and Patton identified four types of triangulations: (a) method triangulation, (b) investigator triangulation, (c) theory triangulation, and (d) data source triangulation.

Method triangulation includes the use of multiple methods to collect data. Investigator triangulation involves the participation of two or more researchers in the same research. Theory triangulation involves the use of different theories to conduct research analysis and subsequent interpretation of data. Data triangulation concerns the collection of data from different people, individuals, and groups (Carter et al. 2014.). Triangulation enhancement for this research study will be through data source triangulation.

The collection of data will be from multiple data sources. The different data sources in this research study are the different cybersecurity managers with the uniqueness and dept of their experiential knowledge. Semistructured face-to-face and telephone interviews will occur with individual study participants. Group interviews will not occur with research participants because of the potential risk of violating the privacy of participants. In addition, a group interview could lead to the distortion of experiences described by study participants when they listen to each other.

Further credibility enhancement will be through member checking (Anney, 2014). Anney (2014) believed that member checking helps to remove the researcher's bias during the analysis and interpretation of data. Interested participants will receive a copy of the transcribed interview data, for necessary evaluation of the researcher's interpretation of the collected data. There will be corrections for any misrepresentation of participants' views, following the feedback from participants (Carter et al., 2014). Peer-reviewed literature, reviews from my dissertation committee, and external peer debriefing will be other credibility enhancements to my research study (Anney). The use of a reflexive journal will aid the avoidance of researcher bias as the researcher acts as the research instrument for the study (Cope, 2014).

Transferability

Houghton et al. (2013) posited that transferability means the findings of the study should apply to other settings—other comparable contexts. Cope (2014) claimed that the findings of the study must have meaning to people who are not involved in the study. Shenton (2004) believed that the researcher must provide enough contextual information about fieldwork sites and data gathering, to enable readers make the contextual transfers themselves. Anney (2014) stated that transferability is "the degree to which the results of the qualitative research study can be transferred to other contexts with other respondents" (p. 277). The facilitation of transferability by a researcher involves thick description and purposeful sampling. Anney suggested that thick description involves the provision of rich and detailed descriptions by the researcher concerning the study and the participants. The use of concept map diagrams and charts, through the Microsoft Excel application,

would provide visual information about research participants. The concept map diagrams would display the demographic information, geographical location, and other appropriate information about participants. Further thick description regards the provision of detailed information about the research methodology and contextual information. The use of purposeful sampling to select study participants would also enhance transferability (Anney).

Dependability

Dependability refers to how dependable and stable the research findings are over time (Bitsch, 2005, p. 86). There is a relationship between dependability and credibility and data source triangulation, which stipulates that research data must be collected from multiple credible sources can positively affect credibility and dependability. Peer examination, like member checking, enhances and contributes to the dependability of the research study (Anney, 2014). The discussion of the research design, process, implementation, and results, with neutral individuals also helps dependability. These neutral individuals are people with experience in qualitative research. The injection of the feedback from them into the research study will enhance dependability. Specifically, the researcher should discuss honestly and in detail the research design and its implementation. The discussion would help people reading the research report to have a thorough understanding of the research method used. Shenton (2004) believed that researchers must provide specific operational details of what occurred in the field concerning data gathering and recommended a reflective appraisal of the research project.

This will help the evaluation of the effectiveness of the process employed in the research inquiry. Confirmability is another criterion to ensure qualitative research trustworthiness.

Confirmability

Confirmability refers to the capacity to which participants can validate and authenticate the correctness of the collected data, as well as the internal coherence of the collected data, its interpretations, and findings. Confirmability concerns the extent to which the researcher can demonstrate that data analysis and interpretations of data are not the biased views of the researcher. Analysis of the interview data should represent the viewpoints of the research participants (Polit & Beck, 2012). The inclusion of the viewpoints and direct quotes from the interview participants represent emerging themes, and should satisfy this requirement (Cope, 2014). Triangulation and reflexive journaling would also help to promote confirmability (Anney, 2014). My reflexive journal will include all events that occur on the field and my reflection about the study.

Ethical Procedures

I will employ several precautionary methods to ensure that the treatment of study participants is ethical. The first step in the process is to ensure that the Walden University IRB approval precedes any interaction with study participants. Application to the IRB with all required documentation and information would jumpstart the approval process. The receipt of the IRB approval number, when it becomes available, would confirm the authorization to proceed. Equally important is that the informed consent form be sent to the participants and must come back in the affirmative for a participant to participate in

the study. All recruitment materials and processes will follow the Walden University IRB procedure.

Data collection intervention activities will include the addition of prequalified study participants from a pool of initially selected participants, in case any participant withdraws from the study. Data collection will be anonymous. There will be no sharing of the names of research participants. There will be a small monetary incentive to participants for agreeing to take part in the research study.

Summary

Chapter 3 consisted of a restatement of the purpose of the research study, the research design, and the rationale, which contained a statement of the central research question. Chapter 3 provided a brief discussion on the research methodology and approach, the phenomena of interest, and the fundamental concepts of the study. I discussed my role as the researcher, and covered ethical research issues, researcher biases, how to manage them, and justification for the use of incentives. Further discussion included a detailed explanation of the participants' selection logic, the structure of the study population, and the sampling strategy. The sampling strategy explained the drawing of the sample from the study population. The discussion on the participants' selection logic included a specific explanation on participants' identification and recruitment. The discussion on the Walden University IRB process provided clarity that no communication with study participants would occur until the receipt of IRB approval. This chapter presented the data collection methods and techniques, the data instrument, and subsequent data analysis. The discussion on research trustworthiness highlighted the four

criteria that will resolve the issues of trustworthiness. Chapter 3 ended with the discussion of the ethical research procedures, which included the treatment of human participants, and intervention activities in case any participant withdraws. A discussion on data collections, analysis, and results will take place in Chapter 4.

Chapter 4: Results

Introduction

The purpose of this descriptive phenomenological study was to explore the lived experiences of cybersecurity managers who have adopted new security laws, new applications, and the IoT to protect users' privacy in the metro areas of Washington, D.C., Maryland, and Northern Virginia. The overarching research question that reflects the purpose of this descriptive phenomenological study was: What are the lived experiences of cybersecurity managers adopting new security laws, new applications, and the IoT to protect users' privacy in the United States?

Chapter 4 begins with a review of the purpose of the study and a restatement of the research question. The discussion on data collection includes the number of participants from whom data were collected, the frequency and duration of data collection, the data collection instrument, and the recording of data. The focus of the data analysis discussion is on the inductive movement of data from coding to categorization to the theming. There is a specific description of codes, categories, and themes that emerged from the data collected from participants. Next is a presentation of the evidence of trustworthiness, which includes the implementation of credibility, transferability, dependability, and confirmability strategies. The summary includes the main points of the chapter and a transition statement to Chapter 5.

Setting

The research setting for this study was affected by the COVID-19 pandemic, which did not allow for data collection through face-to-face and focal group interviews.

In Chapter 3, I stated that data collection would be through semistructured face-to-face and telephone interviews. Additionally, focus group interviews were part of the data collection plan to be used with my previous population (i.e., the youth) before it changed to cybersecurity managers. However, I was unable to use these data collection methods. I had to resort to the use of contactless data collection methods through telephone and Zoom audio and video interviews. Consequently, no discussion on research setting concerning the scenes of interviews and personal conditions influenced participants.

Equally, there was no interaction with any organization other than the posting of recruitment flyers on public social media platforms approved by the IRB for participant recruitment. No organization was involved directly with data collection. Consequently, no organizational conditions could affect the interpretation of study results or influence participants or their experience at the time of the study.

Demographics

The only requirement for participants was a minimum of 5 years of experience as a cybersecurity manager, which was stated clearly on the recruitment flyer. Age and gender identification was not a requirement for this study. The experience of participants ranged from 5 to 25 years; four of the 16 participants were former cybersecurity managers who now work in academia as cyber and information security professors. Three participants were chief information security officers, and others were experienced cyber and information security professionals. All participants had cybersecurity certification that ranged from certified authorization professional, certified information security

management, or certified information systems security professional. The participants came with depths of lived experiences valuable to the research study.

Data Collection

I did not begin recruitment of participants until I received IRB approval. The population for this research study was cyber and information security managers in the metro areas of Washington, D.C., Maryland, and northern Virginia. There were 16 study participants who were interviewed via telephone and Zoom audio and video interviews.

I allotted 4 weeks for data collection; however, it took over 3 months to accomplish. Recruitment of participants took longer than expected and participants' time requirements also stretched the duration of data collection. The duration of each participant's interview was between 30 and 60 minutes. Before finalizing the interview protocol, I followed member-checking procedures by sharing the interview questions with my dissertation committee. The incorporation of their feedback led to the development of an approved interview protocol. This approved interview protocol with open-ended questions guided the process of each data collection event.

The interviews were conversational, and I began the interviews by introducing myself and the study. Brinkmann and Kvale (2015) instructed that an interviewer should (a) be conversational, (b) begin the interview by introducing oneself and the research study, (c) provide the reason for conducting the study, (d) explain why the research is of interest to the study population, (e) inform participants of the length of the interview, (f) assure anonymity, and (g) request participants' permission to audio record the interview. Finally, a researcher should remind participants they may decline any question they do

not wish to answer (Brinkmann & Kvale). All these steps guided the conduct of each interview during data collection.

The collection of data and subsequent transcription and analysis revealed a need for follow-up interviews. As I was transcribing one of the interviews, I needed to contact a participant for clarification in a short follow-up interview. Evidence-based interview practices for increasing representation and legitimation should be used (e.g., member checking interviews; Lincoln & Guba, 1985) including debriefing interviews (Onwuegbuzie et al., 2012). I followed all these guidelines as I collected data.

I did not stop collecting data until I reached data saturation. I reached data saturation when I had collected information from participants that was enough to replicate my study (Fusch & Ness, 2015; O'Reilly & Parker, 2012; Walker, 2012). After my 10th interview, I was no longer receiving new information from participants; all responses were identical to the information I had received from other participants interviewed earlier. I emailed my committee and reported not receiving any new information and requested to stop conducting additional interviews. The committee directed me to complete the interviews with the remaining participants in case any new information should arise. Fusch and Ness (2015) and Guest et al. (2006) explained that data saturation is reached when the researcher is no longer receiving new information and when the fulfillment of collecting any new information from participants has been attained.

I purified the data through bracketing, which is a requirement for descriptive phenomenology. Georgi (1997, 2009) approved the collection of lived experiential

descriptions from participants and subsequently purifying the data procedurally through bracketing. Georgi posited that bracketing is a way for researchers to suspend their previous knowledge about the phenomenon so that biases are removed. I achieved this by suspending my prior knowledge and experiences concerning the protection of users' data and privacy as a certified data privacy solutions engineer. Suspending prior knowledge about the phenomenon falls in line with Husserl's (1970/2012) phenomenological principle. I followed these guidelines from Georgi and Husserl to ensure any preconceptions that may have negatively impacted the research outcome were mitigated. Additionally, I stayed away from the pedestrian public views about data security laws, applications, and the IoT, which are major parts of the phenomenon being studied. Consequently, the uncorrupted and undiluted data collected from participants represented the bedrock of data analysis without the injection of extraneous information.

Data Analysis

I began the process of data analysis by combing through the data collected until I arrived at meaningful answers to the research question on the adoption of new security laws, new applications, and the IoT by cybersecurity managers to protect the privacy of users. Data analysis should begin during data collection (Nowell et al., 2017; Pope et al., 2000). As I interviewed participants, I manually recorded data convergences that represented similar responses from participants along with patterns and themes that emerged from participants. One such example is the issue of privacy concerning the use of IoT devices. A handful of the participants agreed that users must make a choice

between invasion of their privacy and the convenience of using IoT devices. Participant 5 stated,

> At first, I was saying I don't need these smart devices. Now I know I need them. First, is the convenience factor; fortunately, or unfortunately, what am I willing to give up because of the intrusion into people's privacy? All these data that IoT device vendors and organizations take; they will not want to give it back. Organizations don't give up power easily unless there are laws that will compel them to respect people's privacy. The question is, do I want the convenience, or do I want to have the privacy—where is the line I need to navigate? You can't have both. Where is that line that I am willing to cross in compromising my data?

I used inductive reasoning as I analyzed participants' interview transcripts concerning their perspectives on the adoption of data security laws, applications, and the IoT by cybersecurity managers to protect users' privacy. Lincoln and Guba (1985) posited that researchers can use inductive reasoning in identifying patterns in collected data to understand the perspectives of participants. Yilmaz (2013) stated that interpretation and the subsequent understanding of data by qualitative researchers may be done through inductive reasoning. The use of inductive reasoning assisted me in the categorization of data into themes that emerged from the interview data. Inductive reasoning also facilitated the understanding of how cybersecurity managers adopt the keywords in the central research question to protect the privacy of users.

Data analysis is integral to the understanding of field data in qualitative research and one of the critical steps in a research study (Leech & Onwuegbuzie, 2007). Data

analysis facilitates the understanding of interview data from multiple participants to develop themes that provide answers meaningful to the research question. Onwuegbuzie et al. (2012) posited that the use of data from multiple sources (e.g., participants) helps researchers to understand the phenomenon being studied more deeply. Data source triangulation is based on the time of data collection, the space in which data are collected, and the people from whom data are collected (Denzin, 1970; Thurmond, 2001). In this study, data were collected from multiple participants who were interviewed at different times. I was unable to use triangulation (Jia et al., 2021) through a focus group due to the prevailing COVID-19 pandemic situation at the time of data collection. However, the multiple participants with unique experiences in cybersecurity who were interviewed yielded rich data to be analyzed in this study.

I ensured the anonymity of participants as I began to analyze data. To maintain privacy, participant names were replaced with letter/word-number pseudonyms and names were not used at any point in the ongoing analysis of data and subsequent discussions. Participants were only referred to with the number assigned to them. The first participant interviewed was assigned *Participant 1*; the second participant as *Participant 2,* through to *Participant 16*, who was the last participant interviewed.

I used coding in this research study to search for data convergencies, patterns, and relationships. Saldaña (2016) believed that coding data is essential to the research process, and data analysis should begin with coding. My coding process facilitated the understanding of the underlying meanings of the data collected. Rubin and Rubin (2012) recommended seven steps for the analysis of data, including transcription and

summarization of the interview transcript. I adapted and customized these steps sequentially into the following data analysis activities:

1. Read interview and field notes and familiarized myself with the data collected.
2. Viewed and listened to interview recordings and transcribed the data collected.
3. Compared transcribed data with notes; summarize and merged data for completeness.
4. Developed nodes in NVivo and imported transcribed data into nodes.
5. Generated codes that represented the data and the primary research question.
6. Utilized codes that emerged to identify patterns, relationships, and themes.
7. Conducted categorization of codes to develop themes that are in alignment with the research question.
8. Continued the coding process to answer the research question until no new codes and themes were found.

I used NVivo, a computer assisted QDA software for data analysis in this study. However, before the final decision to use NVivo, I conducted a comparison of NVivo with other QDA software. In the comparative analysis, I looked at five QDA software, including NVivo from the Boston University qualitative software comparison presentation (Boston University, n.d.). The QDAs were: NVivo, Atlas.ti, HyperResearch, Dedoose, and Coding Analysis Toolkit (CAT). Of these five, NVivo, Atlas.ti, and HypeResearch were local to the user, which means users' can install the program on their laptop or desktop. Access to Dedoose and C.A.T. are only from a Web location, which means a user may have to be on the Web to enjoy their full functionality. The first three

software do not have this limitation. Although C.A.T. was open source, which means it can be downloaded free of charge, customer support availability was low to none per the publication. When it came to Dedoose, it was inferior in documentation quality, which resulted in the elimination of C.A.T. and Dedoose. A look at hyperResearch, which was one of the top three that revealed it did not support in-depth text queries and the incorporation of response spreadsheets. For those two reasons I dropped hyperResearch. The last two were NVivo and Atlas.ti. Although Atlas.ti has a good business model, it is good with documentation quality and great in intuitiveness, it had limitations. The limitations were the slowing down of videos that need transcribing, because it does not allow researchers to incorporate spreadsheet of participants' responses and does not support the running of in-depth text queries. NVivo, on the other hand, was particularly good in all the considered areas; hence, it ended being the preferred CAQDAS software for my data analysis in this research study. The discussion that follows presents the functionalities of NVivo as a CAQDAS.

NVivo is one of the major CAQDAS available to researchers for the analysis of qualitative data. QSR International (2019) defined NVivo as computer software that is used to support the qualitative and mixed-methods research inquiries and is designed specifically to handle nonnumeric data. The software provides various capabilities to qualitative researchers for collecting, organizing and analyzing data from interviews, various forms of focus group discussions, surveys, audio, social media data, YouTube videos, and web pages. NVivo has all the attributes described above and provides capabilities for data organization and management. First, it has embedded powerful

search tools, visualization, and query capabilities through which data can be organized and effectively managed. With NVivo, a researcher can import various types of data and then organize the data by using various in-built search and query tools within it. NVivo uncovers data connections that are similar and highlights them for necessary grouping. NVivo then gives a code name through which all data representing a theme can go with the appropriate code name. Every connected data to the code can then be categorized and stored in a container or node named with the code assigned to the category. NVivo can be used to organize data. Concerning data management, NVivo supports the preparation of reports, papers, extracts, and presentations, as well as the storing and the retrieval of data. It supports teamwork through team collaboration capabilities. These are to mention a few of the data management capabilities of NVivo as a QDA software. Because of these comparatively superior capabilities, NVivo was my preferred data analysis software program for this study.

Data analysis in NVivo started by importing 16 rigorously transcribed interviews into NVivo for data organization and management. Ten codes that corresponded to the ten questions in the interview protocol were used to create parent nodes in the latest version of NVivo (i.e., NVivo 2020). I read each line in the transcribed interviews manually and coded contextually to the main nodes listed below. Specifically,

- Q01. Navigating adoption data security laws;
- Q02. Describe IoT, navigating adoption;
- Q03. New applications IoT affects privacy;
- Q04. Experiences protecting cyberspace services;

- Q05. Navigate regs, contradictory global legislations;
- Q06. Protecting personal data, privacy;
- Q07. Challenges interconnection of devices;
- Q08. Differences cloud-based, on-premises;
- Q09. Zero-day attack aka zero-day vulnerability; and
- Q10. How cybersecurity info can be provided to users.

These main node names were shortened to avoid truncation in the software program. Woods et al. (2015) asserted that NVivo assists researchers in developing codes and themes that are accurate and representative of the data because it facilitates the in-depth searching of the imported data. As I read and searched through the content of the imported transcribed interview data in NVivo, I conducted the refinement of codes within the nodes. Nodes are data containers that are created in NVivo into which transcribed data are first imported for coding. The refinement of codes led to the creation of 10 coding reports with 192 subcategory codes that were related to the participants' perspectives as they provided answers to the interview questions. A few of the codes are discussed below.

In the first coding report, which was for question one (Q01), Participant 5 stated in answer to the adoption of data security laws under the code "Drives contracts" that "New data security laws drive contracting." He explained that "My company and others will bid on a contract; for companies to be compliant with security laws, they have got to get their personnel trained to be able to be compliant with the laws." This has led to organizations making deliberate efforts to ensure they are compliant.

In Q02 under the question *How have you navigated the adoption of the IoT to protect users' privacy?* Participant 6, under the code "Access codes and protocol" stated that

> Approach to protecting users is by limiting our network access as much as possible. Everything that is allowed to be connected to the network must go through manual review before it can be connected to the network. We use VPN (Virtual Private Networks), encryptions etc. and there are levels of restrictions placed on users. We also limit things that are allowed to be connected to our network. Most IoT stuff are not allowed to be connected to the network. Also, we do not allow users to connect wirelessly without organizational authentication.

In Q03, that explored how new applications in IoT affect privacy, Participant 2 under the code "Compliance and standards" stated that

> So, when you have the new application, the only way to make sure that those applications are good for the consumer is to have standardization where the industry itself will have some level of authority to enforce it. It is like we are not going to do business with you if you don't follow the standard. For example, look at applications (Apps) in the Apps store or the Google play; you cannot add your own app unless it goes through certain standards. And those standards must go through the security before apps are added. We need something like this one, … Additionally, we also need to follow the three pillars, which is, is it secure? Is it safe? Have privacy issues been considered? Developers of applications must

satisfy these three pillars and I must check mark all three before I can say, use this application.

I conducted a further review of the subcategory codes and searched for patterns and relationships among the codes to develop themes and corresponding subthemes (Branco & Davis, 2020). Frels and Onwuegbuzie (2013) asserted that an in-depth analysis of data leads to the discovery of major themes. Consequently, I performed a further refinement of codes, themes, and subthemes, which led to the development of major themes that aligned with the keywords in my research question. Embedded in these major themes are implied application of the conceptual framework of the study by users. As I conducted this thematic refinement of codes, themes, and subthemes, I also searched for peer-reviewed journal articles that aligned with the key words of my research question and the conceptual framework that were the PMT and cybersecurity awareness influenced these themes.

Evidence of Trustworthiness

In this descriptive phenomenological study, credibility, transferability, dependability, and confirmability were used to provide evidence of trustworthiness. Trustworthiness in qualitative research, according to Lincoln and Guba (1985), is the extent to which people have confidence in the findings of the research study. It is also the extent qualitative researchers have confidence in their research data (Polit & Beck, 2012). The few pages below discuss the inclusion of the evidence of trustworthiness in this research study.

Credibility

This descriptive phenomenological study sought to achieve credibility through member checking and peer review. Lincoln and Guba (1985) highlighted member checking as a critical technique to ensure credibility in qualitative research. Member checking allows participants to check and confirm the accuracy of the experiential data collected by the researcher. Consequently, I used the technique of member checking to confirm the accurate interpretation of the data collected by allowing participants to verify the credibility and the accurate interpretation of their experiences by the researcher. The experienced cybersecurity experts and professionals that were interviewed provided credible data. The participants have first-hand experiences that are unique and different from other participants. The uniqueness of the data from each participant, until data saturation was reached, guided against the collection of the same data since experiences about the phenomenon studied was different from one participant to the other. A third technique was peer review that allowed for the sharing of the data collected to couple qualitative researchers for a neural and unbiased look at the data collected. The use of these techniques provided a convergence of research credibility elements that confirmed the evidence of trustworthiness.

Transferability

Transferability of a study means the study findings should apply to other settings with comparable contexts (Houghton et. al., 2013). Transferability also requires the researcher to provide an adequate description of the research study so that readers can make an informed decision about transferring the findings of the study to other contexts

(Lincoln & Guba, 1985). Anney (2014) posited that transferability involves the provision of thick description, which involves the provision of rich and detailed data about the study and the participants. In this study, I provided a rich and detailed description of the study and the participants using pseudo names to represent the actual names of participants for anonymity. Additional thick description involves the provision of detailed information about the research methodology and contextual information. The use of purposeful sampling also ensured transferability as evidence of trustworthiness. The researcher recruited participants using purposeful sampling. Purposeful sampling is less restrictive; other researchers could replicate the study by using the same method of sampling to recruit rich cases that have the relevant information being sought. Consequently, the use of thick description, the description of the procedures I followed to conduct the study, and the provision of information concerning participants have provided enough data to help others recreate my study findings and make judgement on my study findings.

Dependability

Dependability refers to how dependable and stable the research findings are over time (Bitsch, 2005). This descriptive phenomenological study achieved dependability as evidence of trustworthiness by using peer examination, member checking, and data source triangulation. Peer examination, like member checking, enhances and contributes to the dependability of the research study (Anney, 2014). The researcher shared transcripts with participants after interviews were conducted for a confirmation of the accuracy of the transcribed data. Feedback from participants were injected into the study.

Equally important, was the sources of data. The researcher collected research data from multiple participants with unique experiences and depth of experiential knowledge concerning the phenomenon being studied. The differences in the experience and knowledge of participants ensures data source triangulation, as many of the participants shared data that were different from other participants until the researcher reached data saturation with no new information being shared by participants.

Confirmability

Confirmability refers to the capacity to which participants can validate and authenticate the correctness of the collected data, as well as the internal coherence of the collected data, its interpretations, and findings. Confirmability concerns the extent to which the researcher can demonstrate that data analysis and interpretations of data are not the biased views of the researcher. Analysis of the interview data should represent the viewpoints of the research participants (Polit & Beck, 2012). To actualize this, I included viewpoints and direct quotes from interview participants. Follow up interviews were conducted with a few participants for the validation and authentication of the correctness of the collected research data.

Results

The overarching research question that reflects the purpose of this descriptive phenomenological study was: *What are the lived experiences of cybersecurity managers adopting new security laws, new applications, and the IoT to protect users' privacy in the United States*?

This section includes a discussion of the five main themes that arose from this study. The discussion encompassed a presentation of the study results from the analysis of the data collected on how cybersecurity managers have experienced the adoption of new security laws, new application, and the IoT to protect the privacy of individuals. The five major themes that emerged from my analysis of data were data security laws and the protection of users' privacy; new application by IoT affects users' privacy protection; the security of IoT devices is essential for IoT adoption; zero-day vulnerability and users' privacy protection; and continuous training is critical to cybersecurity awareness, privacy, and data protection.

Theme 1: Data Security Laws and the Protection of Users' Privacy.

The adoption of data security laws to protect individual users' privacy came directly from the research question. The review of literature in this study revealed that data security laws were enacted to protect the personal information of people. The protection of individual privacy in cyberspace depends on the protection and effective management of the personal data of individuals. Table 1 shows the total count that represents the number of respondents and the reference number.

Table 1

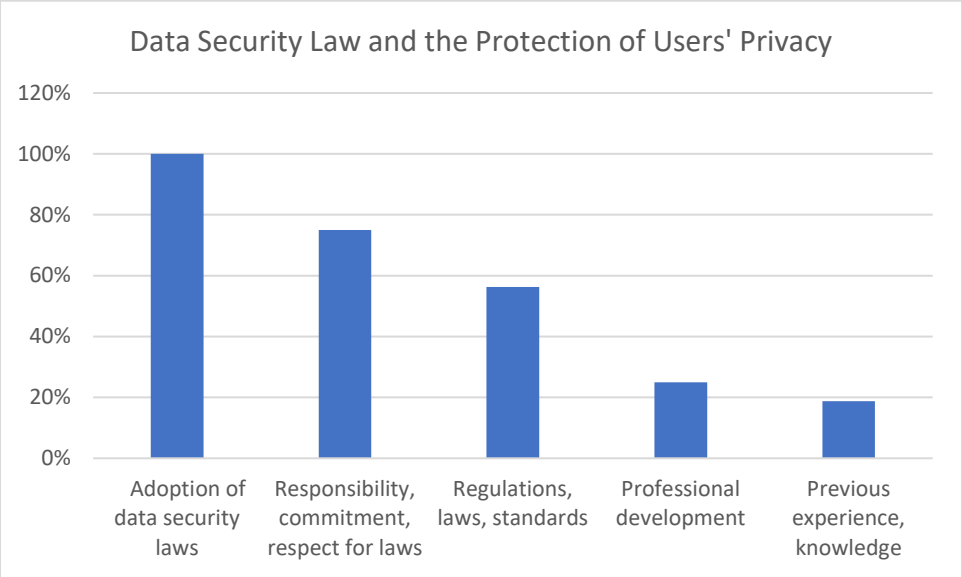
Frequency of the First Major Theme

		Participant
Major theme	Count	References
Data security law and the protection of users' privacy	16	72

Figure 1 shows a distribution of the responses of participants. Twelve participants that represented 75% of data sources concerning the responsibility, commitment, and respect for data security laws, agreed that data security laws were for the protection of users' privacy. Participant 1, a former cybersecurity manager now in academia, explained that she has been able to navigate the adoption of data security laws by ensuring that all her faculty go through training in data privacy every academic year. She stated, "Respect for and adherence to federal security laws is important." Participant 2 indicated that data security laws are important and issuing authorities must publicized the laws for wider adoption. He stated that "we only hear about General Data Protection Regulations (GDPR) and the California Consumer Privacy Act (CCPA) when there is somebody suing due to a violation of the laws." Participant 8, a chief information security officer, whose response cuts across all the categories under this theme as shown in Figure 1, stated that "I am directly impacted by data security laws as I work with the Department of Defense (DoD) and the Federal Emergency Management Agency (FEMA). We collect only the data that we need, and we use NIST RMF Framework Privacy Controls like authority and purpose (AP), administrative controls (AC), data quality and integrity (DI) controls to protect users' privacy."

Figure 1

Data Security Law and the Protection of Users' Privacy



Nine participants who represent 56% of the data indicated that regulations, laws, and standards are important to the adoption of data security laws. Participant 11 stated,

> We follow the NIST RMF and categorize systems that host applications concerning the confidentiality, integrity, and availability levels of the applications on a scale of high (H), moderate (M), and low (L). If one of the three areas of confidentiality, integrity, and availability is H for the application being hosted by a system, the system is categorized as H and appropriate security controls are then sought from relevant NIST publications and the controls are implemented on the system.

Participant 12 stated,

> The general data protection regulation (GDPR) is one of the new privacy and data security laws passed in the European Union (EU), but it impacts any organization

> that provides services to or collect data related to the people in the EU. This privacy law has strict guidance regarding data privacy and security from ensuring protected personal data has the required equals including, but not limited to, encryption at rest and in transit, multifactor user authentication, and appropriate disclosures on how data is collected, used, and stored.

The above responses from Participants 11 and 12 confirmed the relevance of the security choices cybersecurity managers must make in adopting data security laws to protect the privacy of users. Cybersecurity awareness influenced the choices of 25% of participants whose responses focused on professional development and the seeking of knowledge. The acquisition of knowledge would aid a wider awareness about data security laws. This will in turn enhance the adoption of data security laws by cybersecurity managers to protect the privacy of individual users.

Theme 2: New Application by IoT Affects Users' Privacy Protection

The focus of Theme 2 is on how new applications by the IoT affect users' privacy protection and this came out of the research question. The IoT, with the accompanying development of new applications, has introduced serious privacy and security threats to individuals in cyberspace (Fawaz & Shin, 2019). Data collected revealed that the enablement of new applications by IoT and the interactions among interconnected devices have introduced more challenges for cybersecurity managers in protecting users' privacy and their connected devices from the prevailing cyberthreats. Multiple participants indicated that new applications by IoT have led to security challenges and invasion of the privacy of individuals. Participant 1 indicated that it is hard to trust any

application because of the intentions of application vendors. Hahn (2017) provided an explanation about the interception of location data of IoT devices after the installation of third-party applications. Participant 3 stated “the enablement of new applications by the IoT has made the issue of the protection of users’ privacy more problematic.” New application erodes users’ privacy and users become more vulnerable when they download new applications.” Participant 3 described privacy as a home with unlocked windows or doors and asserted that this is what happens because of the download of new applications. Participant 6 stated that “Users’ privacy is constantly being whittled away… the more applications people install through what they use, the more they lose their privacy.” He stated further that “People must decide on their preference (i.e., convenience over privacy or privacy over convenience).” This is a key decision cybersecurity managers and individual users must make. How much of my privacy do I want invaded by installing new applications that are mandatory so that I can use IoT devices and derive comfort from it? There is a choice to be made and this may require further studies. Why do people choose convenience over the privacy of their data and vice versa?

Table 2

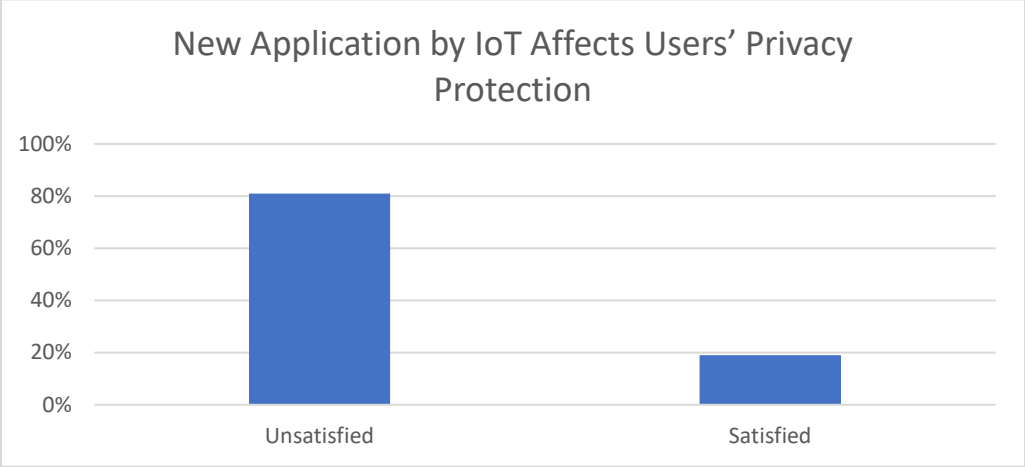
Frequency of the Second Major Theme

	Participant	
Major theme	Count	References
New application by IoT affects users’ privacy protection	16	81

Figure 2 shows that 81% of the participants were unsatisfied concerning the negative effect of new applications that were enabled by the IoT on the privacy of individual users. Only 19% of participants interviewed were satisfied.

Figure 2

Effect of New Applications on Users' Privacy



The majority of the participants who represented an overwhelming 81% (13) of cybersecurity managers made choices that aided the protection of individual users' privacy, as well as their own privacy. Participant 8 indicated that users who use IoT arm sugar monitors had to make some decision on the intrusive personal data request from the manufacturers of the product. This request from vendors also affects users' privacy; users must appraise the threat when the product manufacturer asks about collecting data through the application to ensure their product is functioning right. How a user responds to this threat would be through appraising how to cope or respond to the threat. This leads to response efficacy beliefs from which coping appraisal emanated. Shillair et al. (2015) explained that coping appraisal emanates from response efficacy beliefs, which focuses

on the effectiveness of adaptive responses in resolving threats. The next theme is the adoption of data security laws to protect individual users' privacy.

Theme 3: The Security of IoT Devices is Essential for IoT Adoption

This theme relates back to the research question that sought to know how cybersecurity managers adopted the IoT to protect individual users' privacy. Adoption of the IoT is accompanied by many requirements. A major one of these requirements is the security of the IoT devices. As the analysis of data revealed, multiple participants indicated that IoT is made of interconnected devices. Participant 6 described the IoT "as the ever-expanding network of consumer and commercial products; these are categorized as the IoT products. Before these products were just things, but with the advent of the internet, they are now connected to the Web." Participant 8 described IoT "as the myriad of devices available in the world that have data connection and capabilities. Electronic items that often have some form of processing capability that give some utility to users." Participant 9 described the IoT as the "physical objects that are embedded with sensors, processing ability, software, and other technologies, and that connect and exchange data with other devices and systems over the internet or other communications networks." Table 3 shows the participants count and the references.

Table 3

Frequency of Third Major Theme

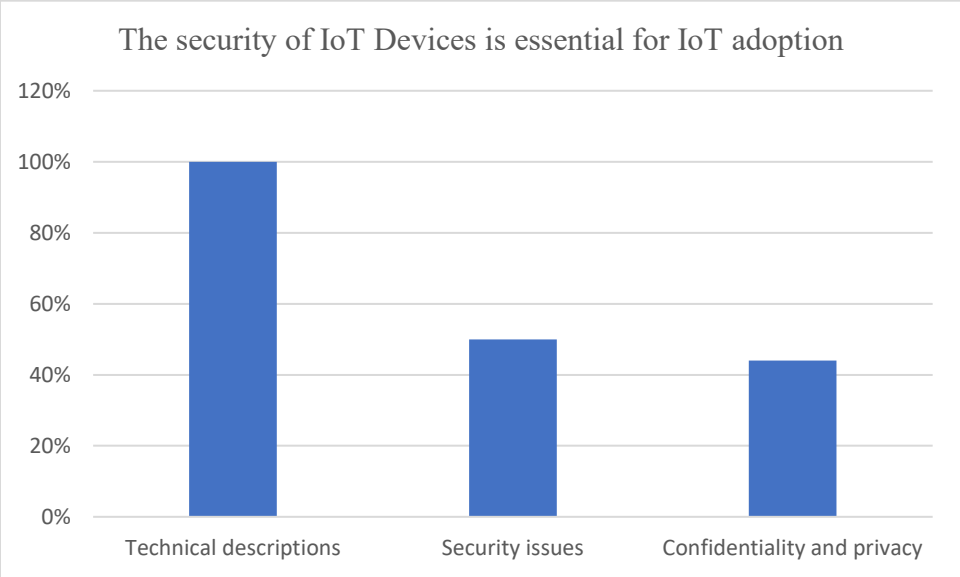
	Participant	
Major theme	Count	References
The security of IoT devices is essential for IoT adoption	16	83

These descriptions by cybersecurity managers confirmed that the IoT is comprised of interconnected devices that have processing capability. The number of these interconnected devices in the IoT keep increasing and may reach “tens of billions” and even “trillion and beyond” (Fawaz & Shin, 2019, p. 40; Ullah et al., 2018, p. 73468).

With this increase comes attending security concerns and challenges; 50% of participants indicated that security of IoT devices is the major impediment to the full adoption of the IoT. Participants 1 stated “when it comes to IoT, assets must be protected. There must be multilayer authentication like access control ….” Balte et al. (2015) found major issues concerning IoT security around access controls and authentication among other IoT security issues. Participant 9 also stated that authentication was a major challenge to IoT adoption and advised users to: “Educate yourself about two-factor authentication.”

Figure 3

The Security of IoT Devices Is Essential for IoT Adoption



The application of the National Institute of Standards and Technology (NIST) security controls for authorization domain protection is one of the good practices by cybersecurity managers to ensure security of devices to protect individual users' privacy. Participants 8 and 9 confirmed the use of security and privacy controls. One such control is the newly created PT, personally identifiable information processing and transparency control family (NIST 800, 53rev5). Nonapplication and enforcement of appropriate security controls and other security measures by cybersecurity managers would result in maladaptive response. Maladaptive response occurs when an individual decides to either do nothing or do something that increases risks. Not changing passwords and using default passwords are examples of maladaptive response. Participant 2 provided an example of a university that used default password and got attacked by cybercriminals.

Theme 4: Zero-Day Vulnerability and Users' Privacy Protection

The findings of this research study revealed that users' privacy can be dangerously affected by zero-day attack (aka zero-day vulnerability). Fourteen of the participants interviewed had a deep understanding of what constitutes a zero-day attack and provided descriptions. Participant 3 stated "A zero-day attack means the system is not available for business use as it has been taken over by hackers or cybercriminals." Participant 4 stated

> A zero-day vulnerability will indicate a time when we are disconnected in a massive way. It means nothing is running on that day. Your zero-day comes when you are not able to conduct business using your IT infrastructure due to the infiltration of hackers or cybercriminals leading to massive vulnerability in the IT infrastructure.

Table 4

Frequency of the Fourth Major Theme

	Participant	
Major theme	Count	References
Zero-day vulnerability and users' privacy protection	16	88

Participant 7 described zero-day attack as an "attack that blindsides the IT security officers, often causing enough confusion where the data that has been accessed is not explicitly clear and therefore a worst-case scenario must be assumed." Participant 12 stated,

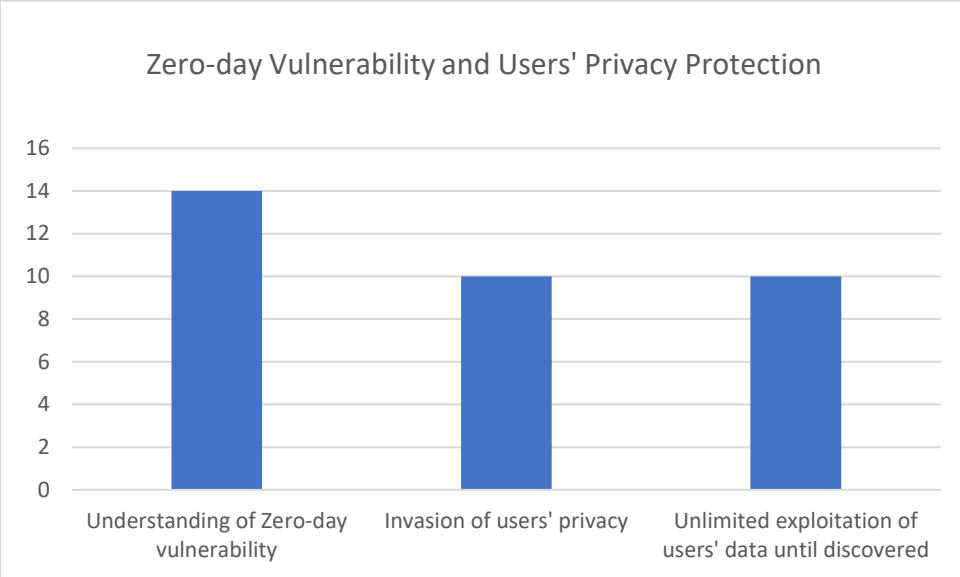
> Just as the name implies, zero-day attacks are launched to exploit unknown or newly discovered vulnerabilities within systems. These vulnerabilities could reside in software codes but were uncovered by attackers before the software manufacturer or vendor releases a security patch/fix.

The discussion represents a cross section of participants' descriptions about their understanding of zero-day attack/vulnerability. Shamsi et al. (2016) confirmed that zero-day attack occurs from zero-day vulnerabilities and the attack can lead to endless invasions of users' privacy and the stealing of personal sensitive data. According to Shamsi et al., the Heartbleed attack of 2014 was a result of "Vulnerability in the Secure Sockets Layer protocol…which was exposed and revealed supposedly encrypted confidential information" (p. 21). Another zero-day attack that affected users' personal data and privacy was the Target store credit-card theft that occurred "from a zero-day vulnerability at the point-of-sale terminals, which was used to steal credit-card information at a large number of Target stores." In Figure 4, 10 participants that represented 63% of the data source confirmed from their experiences that zero-day attack could lead to the invasion of users' privacy. This is the same for the unlimited exploitation of users' data until the vulnerability is discovered and mitigated.

Cybersecurity managers must respond to this threat using two methods: the threat and the coping appraisals, which are performed in tandem in response to a threat. Tsai et al. (2016) posited that both appraisals are responsible for the behavioral intentions of internet users, in adopting protective or nonproductive security intentions to respond to threats.

Figure 4

Zero-Day Vulnerability and Users' Privacy Protection



In response to a threat, individuals engage in a behavior that could either be adaptive or maladaptive in their bid to respond to a threat. Adaptive response is the implementation of good security practices to deter the threat before a full-blown attack takes place. Participants 1and 3 explained that default passwords must be changed, and systems must be patched continuously to avoid zero-day attack. Not patching the system would be a maladaptive behavior in response to a threat like the zero-day vulnerability attack. Cybersecurity awareness could also apply in response to this threat. This is because cybersecurity awareness focuses on the methodical way to educate internet users about cyberthreats and the vulnerability of data and computer systems to these threats (Rahim et al. 2015; Shaw et al., 2009).

Theme 5: Continuous Training Is Critical to Cybersecurity Awareness, Privacy, and Data Protection

As highlighted by theme 5, the need for continuous training is important to cybersecurity awareness. The focus of cybersecurity awareness is on the methodical way to educate internet users about cyberthreats and the vulnerability of data and computer systems to these threats (Rahim et al. 2015; Shaw et al. 2009). Also embedded in the theme is the protection of users' privacy, which is a major part of the research question. Equally important is the protection of individuals' personal data, which if infringed, would lead to the invasion of users' privacy. Personal data protection focuses on the protection of personal data from the invasion of cybercriminals in cyberspace (Broadhurst & Chang, 2013).

Table 5

Frequency of the Fifth Major Theme

	Participant	
Major theme	Count	References
Continuous training is critical to cybersecurity awareness, privacy, and data protection	16	90

Figure 5 confirmed that 88% (14) of the participants spoke about the importance of cybersecurity education and training; 44% (7) of the participants suggested that cybersecurity awareness, privacy, and data protection training must be continuous. Participant 7 suggested that training is helpful and should be administered on a more frequent basis and stated that "I've seen a lot of security trainings offered on a yearly basis; however, I would suggest a quarterly training exercise as security needs change

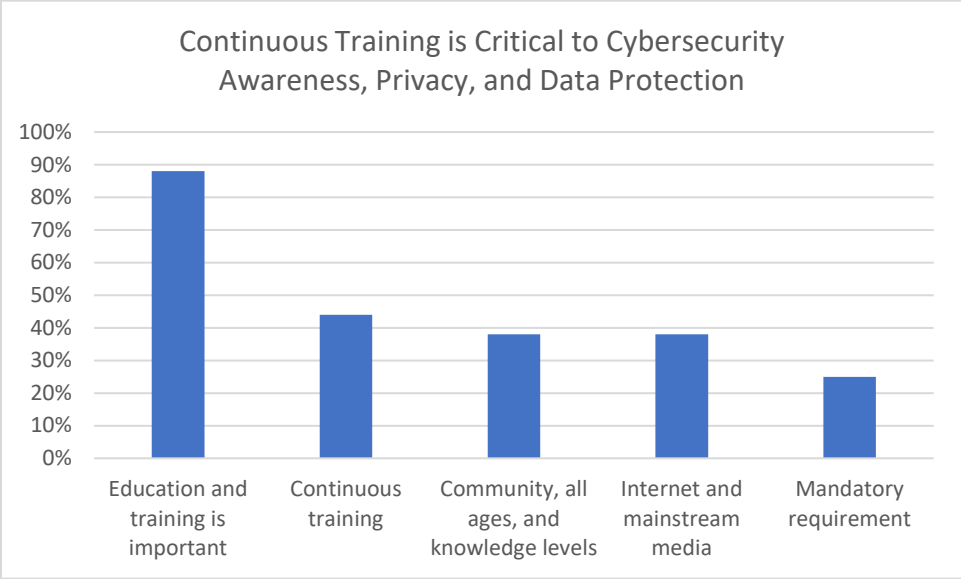
often and rapidly." Participant 2 agreed that training should occur regularly without suggesting a particular cadence; 38% (6) of the participants suggested that training should cover all ages and knowledge levels. Participant 6 stated, "there must be community education for all levels of internet users." Participants 2 and 3 agreed that there are different kinds of internet users, and users of all levels must be educated.

To reach communities of users, 38% (6) of participants suggested that training should be delivered through the internet and mainstream media (e.g., YouTube). This introduces security requirements that must be considered since the training is now open to the public. Participant 2 stated that training the public would require the provision of simple instructions to users on how to secure their computers and added that part of the instructions should include the need to change their default password and the setting up of two-factor authentication. In doing this, the user experience should be considered. Participant 2 further stated, "the more we are simplifying the user interface and making the user experience better, the better for us; but still the security must be there." Participants also suggested that cybersecurity, privacy, and data protection trainings should be a mandatory requirement.

Figure 5 showed that 25% (4) of the participants agreed that cybersecurity education must be a mandatory requirement in schools.

Figure 5

Continuous Training and Cybersecurity Awareness, Privacy, and Data Protection



Participant 6 suggested that cybersecurity awareness education must be made mandatory and not just an elective and stated that "this must be the same way health and physical education classes were mandatory in schools."

Cybersecurity awareness provides the understanding users' need to handle online threats. As previously explained, cybersecurity awareness focuses on the methodical way to educate internet users about cyberthreats and the vulnerability of data and computer systems to these threats (Rahim et al. 2015; Shaw et al. 2009). Appraisals of threats and how to develop coping strategies come with an understanding of cybersecurity, privacy, and personal data protection. This is what continuous training of all kinds and levels of internet users would achieve. Participant 3 stated, "Cybersecurity awareness comes with individual education". This is exactly what the training and education of a diverse population of internet users would facilitate.

Summary

Chapter 4 provided answers to the overarching research question for this study. The first three themes answered the adoption of new data security laws, new applications, and the IoT by cybersecurity managers to protect users' privacy. Theme 1 showed various ways through which cybersecurity managers have adopted data security laws to protect individual users' privacy. Cybersecurity managers agreed that data security laws are critical to the protection of users' privacy. Theme 2 revealed that the adoption of new applications has not been easy as it has led to security challenges and invasion of the privacy of individuals. Data collected revealed that the privacy of users is constantly being whittled away by the installation of new applications and more needs to be done to ensure the protection of users' privacy. Theme 3 revealed that security of IoT devices is the major impediment to the full adoption of the IoT. Cybersecurity managers agreed that individual users who use IoT devices must make conscious and deliberate efforts to protect themselves. They advised users to educate themselves about two-factor authentication to protect themselves. Users must decide between convenience and security that protects the invasion of their privacy.

The other two themes are the zero-day vulnerability and users' privacy protection, and continuous training is critical to cybersecurity awareness, privacy, and data protection. Since a zero-day attack that always results from a zero-day vulnerability affects users' privacy and personal data protection, cybersecurity managers suggested that proactive protective security measures must be undertaken to preempt the occurrence of the attack and mitigate it before harm is done. The last theme that concerns continuous

training to ensure an understanding of cybersecurity awareness, privacy, and personal data protection also focused on an aspect of the research question, which was users' privacy protection. Continuous education of the user base leads to the development of an informed internet user base that will adopt best cybersecurity practices to ensure privacy and personal data protection. Chapter 5 will include discussions, conclusions, and recommendations.

Chapter 5: Discussion, Conclusions, and Recommendations

Introduction

The purpose of this descriptive phenomenological study was to explore the lived experiences of cybersecurity managers who are adopting new security laws, new applications, and the IoT to protect individual users' privacy. The first key finding from the study was that data security laws have enabled the protection of users' privacy. The second finding was that new IoT applications have adversely affected users' privacy protection. The third key finding was that the security of IoT devices is essential for IoT adoption. The fourth key finding was that users' privacy protection can be dangerously affected by zero-day attack (aka zero-day vulnerability). The last finding was that continuous training is critical to cybersecurity awareness, privacy, and data protection.

Interpretation of the Findings

The protection of individual users' privacy in cyberspace has become important due to the unauthorized and manipulative use of individual personal data. The adoption of data security laws, new applications, and the IoT by cybersecurity managers to protect the privacy of individual users has also become important. Brimblecombe (2020) argued that the privacy rights of individuals in cyberspace have become eroded. Consequently, cybersecurity managers must constantly navigate between the adoption of new security laws, new applications, the IoT, and the expanding landscape of technology to protect the privacy of individual users in cyberspace (Brimblecombe, 2020; Pizzolante et al., 2018; Sanchez Alcon et al., 2013).

With the provisions of the conceptual framework for this study—PMT supported by cybersecurity awareness—cybersecurity managers have applied themselves to protecting the privacy of individual users. The PMT mediating process has two appraisal methods: threat appraisals and coping appraisals. Individuals perform these two appraisals in response to a threat. In response to a threat, the PMT explains that an individual engaged in a behavior that could be adaptive or maladaptive. Adaptive responses are good practices that facilitate the mitigation of security and the invasion of privacy risks. Maladaptive responses occur when an individual decides to either do nothing or do something that increases risks. Cybersecurity awareness, as explained in the literature review, focuses on the systematic way of educating internet users about cyberthreats and the vulnerability of data and computer systems to these threats (Rahim et al. 2015; Shaw et al., 2009).

Data security laws have been enacted to protect the personal information of people. The protection of individual privacy in cyberspace depends on the protection and effective management of individual personal data. One of the findings in this study was that data security laws have enabled the protection of users' privacy in cyberspace. Cybersecurity managers confirmed from their lived experiences that the application of the existing and new data security laws has enabled the protection of individual users' privacy. This is contrary to previous literature in which researchers explained that the attempt to put data security laws in place to protect the privacy of individual users has not protected the privacy of users as expected. Purtova (2018) argued that the personal data of individuals closely related to the protection of their privacy would continue to grow,

and its application could expand to an array of diverse meaning and interpretation. Another consideration is the emerging changing interpretation of the concept of personal information in the IoT due to the "exploding generation and aggregation of data, as well as advances in data analytics" (Purtova, 2018, p. 41). Despite these prior assertions concerning the difficulty in protecting individuals' personal data that ensures their privacy protection, the findings in this study confirm that the application of data security laws by cybersecurity managers has enabled the protection of users' privacy.

In the literature review, I found that new applications that have been enabled by the IoT have introduced serious privacy and security threats to individuals in cyberspace (Fawaz & Shin, 2019). Compounding the problem is the increasing number of interconnected devices in the IoT, which have enabled the development and introduction of new applications. The finding from this study revealed that new applications that have been enabled by the IoT have negatively affected users' privacy protection. This finding confirmed the previous literature.

The security of IoT devices that continues to drive the adoption of the IoT is important. The number of devices that constitutes the IoT continues to grow with increasing security problems. The review of the literature revealed that the number of end-users connected devices in the IoT may reach "tens of billions" and even "trillion and beyond" as the adoption of IoT increases (Fawaz & Shin, 2019, p. 40; Ullah et al., 2018, p. 73468). Not only is the increase in the number of IoT devices a problem, the interactions among these interconnected devices with different operating systems, software platforms, and applications also pose a threat to the full adoption of the IoT.

This has introduced more challenges for cybersecurity managers in protecting users' privacy. The finding from this study revealed that the security of IoT devices continues to be a challenge to the full adoption of the IoT. This finding aligns with the literature. Cybersecurity manager participants indicated it has been difficult to protect IoT devices; multiple managers indicated they do not allow IoT devices to be connected to their corporate networks.

Compounding the problem further is the behavior of individual users. In the literature review, I found that despite the layers of information security mechanisms in place, human factors, including individual user behavior, may affect the protection of privacy and personal data in cyberspace (Öğütçü et al., 2016). Users must decide between the convenience and benefits of using IoT devices and the persistent invasion of their privacy that accompanies this use. PMT highlights the behavioral intentions of individual users. Whether a user prefers convenience of using IoT devices over the invasion of their privacy is a decision every user must make. In making this decision, PMT presents two appraisal methods: threat appraisals and coping appraisals. Individuals must perform these two appraisals in the assessment of their need to engage in a behavior in response to a threat. These two appraisals are responsible for the behavioral intentions of internet users in adopting protective security intentions to protect themselves while interacting in cyberspace (Tsai et al., 2016). Inversely, a user could also decide that the benefit of using IoT devices outweighs the invasion of privacy and choose a maladaptive response to the threat, which means they decide to do nothing concerning securing their privacy (Rogers, 1975, 1983).

In this study, cybersecurity manager participants confirmed a threat to the privacy of individual users from zero-day attacks or zero-day vulnerability. Findings revealed that users' privacy is negatively affected by such an attack due to the erosion of personal data. Cybersecurity managers have a deep understanding of what zero-day vulnerability is and the damaging effect it has on the protection of users' data and privacy. Shamsi et al. (2016) confirmed that zero-day attacks occur from zero-day vulnerabilities and the attack can lead to endless invasions of users' privacy and the theft of sensitive personal data. The Heartbleed attack of 2014 revealed users' confidential information, and the Target store point-of-sale terminal attack led to the theft of credit card information for several users, confirming that user information is usually targeted (Shamsi et al., 2016).

The training and education of internet users is important in establishing an informed and educated user base. The final key finding in this study is that continuous training is mandatory and critical to user awareness of cybersecurity, privacy, and data protection. Cybersecurity awareness is the supporting conceptual framework for this study, and the focus is on the methodical ways of educating individual internet users about cyberthreats and the vulnerability of data and computer systems to these threats (Rahim et al. 2015; Shaw et al. 2009). Cybersecurity awareness offers an important defense in the protection of systems and people. Cybersecurity awareness encompasses understanding and knowledge concerning individuals' apprehended dispositions, behaviors, and the connection that exists among them (Chanderman & Van Niekerk, 2017). In the literature review, I found that cybersecurity managers are concerned about the misalignment in the levels of cybersecurity knowledge and the awareness of people

whose privacy they are supposed to protect. This last finding confirms the assertions in the literature review that training internet users will aid in cybersecurity awareness and facilitate the protection of individual users' privacy. Above all, targeted cybersecurity awareness campaigns that address the weaknesses of specific populations of internet users are necessary to protect individual users' privacy.

Limitations of the Study

This study followed the qualitative research methodology, which limited the study due to the relative weakness of the method. The use of purposeful sampling to select research participants made study participants not adequately representative of the population. However, this did not impede the relevance of the study as purposeful random sampling (Patton, 2015) was used to mitigate this risk. The 16 participants who were recruited for the study from the Washington D.C., Maryland, and the Northern Virginia metro areas may seem not representative nationally; however, I deliberately recruited participants that had the rich data that was required for the study.

Contrary to what I stated in Chapter 3 concerning the collection of data, which was planned to be through face-to-face interviews, I was only able to collect data through the Zoom video/audio and telephone interviews due to the COVID-19 pandemic. Equally important is the quality of the data collected because research is only as good as the quality of the data collected. The use of only interviews as the method of data collection could introduce limitation to the study. To mitigate this, I used data source triangulation by collecting data from multiple data sources. The use of multiple methods to collect data should be considered in future research studies of this nature.

My role as the researcher did not introduce limitations to the research in terms of biases. I ensured there was no personal and professional relationship with any of the study participants. I did this to ensure I guarded against any form of bias. Equally important were biases from participants. I made conscious efforts to guide such biases and prejudices during the interview sessions and the analysis of data.

Regardless of these limitations, the related interpretations and the result of this study could still be used as a foundation for future research studies concerning the exploration of users' awareness in cybersecurity, and the protection of users' privacy and personal data.

Recommendations

Recommendations are a part of the outcome of research studies since not all areas can be covered by one study. There could be new data that are collected during data collection that was not part of the focus of the current study. These scope creeps usually end up under the recommendation for future studies. This actionable new data that are discovered during data collection should be examined to generate additional data that would enrich the current data-gap in this field of research endeavor. The focus of this study was on the exploration of cybersecurity managers' experiences in protecting users' privacy and only used one method of data collection, which was interviewing. It is recommended that additional methods of data collection (e.g., focus groups, observations, and documents) should be added to interviews in collecting data for further research in this same topic area.

Secondly, the current study used the qualitative research methodology. It is recommended that the quantitative research methodology should be used to investigate the effectiveness of cybersecurity managers protection of individual users' privacy in cyberspace. Further research data enhancement could also occur using a mixed-method research methodology.

Thirdly, there is an area of the IoT device invasion of the privacy of individuals involving implicit consent. This was part of the data collected from the field. The IoT doorknob that has an embedded camera captures the image of a delivery person who comes to deliver a package at the door. The delivery personnel would not know he is giving his image that has been captured by the camera in the doorknob. This picture has been taken and may be used without any consent given by the delivery person. By working to the door to deliver the package, his consent is implied. There is still no law that states that homeowners with IoT doorknob should display a notice by their door that the doorknob has a camera and by coming into that premises, you are given your implicit consent for your picture to be taken and could be used as a computer desktop or end up on Facebook. One question is, how many people have had their privacy invaded through implicit consent? Another question is, who owns this data that is given by implicit consent enabled by new applications driven by the IoT? There is a whole new area that takes this privacy issue to another level, and there is need for research in this area.

Another area for further research is the behavioral intentions of individual users who choose a maladaptive response to the threat of the invasion of privacy due to the benefit or convenience of using the IoT devices. Security is important and invasion of

individuals' privacy should be discouraged. The question is, what makes a user choose convenience over security and the invasion of his/her privacy? Could it be due to the lack of cybersecurity awareness? This is an area that requires further investigation.

Implications

The findings from this descriptive phenomenological study might contribute to positive social change by yielding valuable research data that are useful to the development of cybersecurity policies and strategies aimed at protecting the privacy of individual internet users. Individuals benefit by personalizing the findings to make positive, life-changing decisions through the application of these findings. One such benefits is a decision for continuous training that is critical to the acquisition of invaluable knowledge in cybersecurity awareness, privacy, and data protection. Since family units consist of individuals, families benefit directly from the positive social change choices that are made by individual members of the families.

Organizationally, business managers are now armed with more information on how best to protect data and privacy. Governments now have the data to legislate appropriate laws that would aid the protection of personal data and individual users' privacy in cyberspace. Equally, educational institutions are equipped with the data to develop relevant curriculum that will increase the knowledge of the internet user base.

The findings from this study helps to improve the practice of cybersecurity around privacy protection. The findings equip cybersecurity managers and other organizational IT leaders with the data to build practices that facilitates the faster adoption of data

security laws, applications, and the IoT to protect individual users' personal data and privacy.

It is recommended that leaders in the IT industry and cybersecurity managers should adopt a culture of continuous training to establish an educated internet user base. It is also recommended that the annual cybersecurity awareness training and other security trainings should change to quarterly. There is a need to introduce the change gradually; this may begin through a semi-annual approach with the ultimate end goal of making it quarterly. The protection of users' data and privacy is critical to a data-centric healthy workplace. This explains the aggressiveness in terms of the recommended change to quarterly offering of the trainings. This also helps to reinforce the knowledge acquired from the contents of the training for better cybersecurity practice. Finally, there should be a review of the current user educational curriculum for an injection of necessary changes that align with the findings of this study.

Community training of internet users is also important. Not all internet users are within the four walls of an office or schools. The findings of this study will be useful to community leaders and other IT stakeholders in developing a plan to address the continuous training needs of various communities of internet users.

Conclusions

Navigating the adoption of data security laws, applications, and the IoT by cybersecurity managers to protect individual users' privacy was the focus of this study. The findings from the study suggest that data security laws have enabled the protection of users' privacy. Regardless, new applications that have been enabled by the IoT have

negatively affected users' privacy protection. The security of IoT devices is found to be essential to the adoption of the IoT, but the behavior of individual users still stands in the way of quick and full adoption of the IoT. User training continues to be critical to the acquisition of knowledge in cybersecurity awareness, privacy, and data protection.

This study has provided a veritable window to look at the adoption of new technologies. Through this study, governments, organizations, and individuals now have actionable research data that will guide the review of existing IT requirements for needed changes. The study also fills a gap by adding to the existing data in this area of research.

References

Aagaard, J. (2017). Introducing post-phenomenological research: A brief and selective sketch of phenomenological research methods. *International Journal of Qualitative Studies in Education*, *30*(6), 519–533. https://doi.org/10.1080/09518398.2016.1263884

Abawajy, J. (2014). User preference of cybersecurity awareness delivery methods. *Behavior & Information Technology*, *33*, 237–248. https://doi.org/10.1080/0144929X.2012.708787

Akhyari, N., Ruzaini, A. A., & Rashid, A. H. (2018). Information security culture guidelines to improve employee's security behavior: A review of empirical studies. *Journal of Fundamental and Applied Sciences*, *10*, 258–283. https://doi.org/10.4314/jfas.v10i2s.21

American Psychological Association. (2009). *American Psychological Association publication manual.*

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, *34*(3), 613–643. https://doi.org/10.2307/25750694

Annells, M. (2006). Triangulation of qualitative approaches: Descriptive phenomenology and grounded theory. *Journal of Advanced Nursing*, *56*(1), 55–61. https://doi.org/10.1111/j.1365-2648.2006.03979.x

Anney, V. N. (2014). Ensuring the quality of the findings of qualitative research: Looking at trustworthiness criteria. *Journal of Emerging Trends in Educational Research and Policy Studies (JETERAPS)*, *5*, 272–281.

Atkinson, S., Furnell, S., & Phippen, A. (2009). Securing the next generation: Enhancing e-safety awareness among young people. *Computer Fraud & Security*, *2009*(7), 13–19. https://doi.org/10.1016/S1361-3723(09)70088-0

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019). Americans and privacy: Concerned, confused, and feeling lack of control over their personal information. *Pew Research Center*. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, *84*(2), 191–215. https://doi.org/10.1037/0033-295x.84.2.191

Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory.* Prentice-Hall.

Bell, J. S. (2002). Narrative inquiry: More than just telling stories. *TESOL Quarterly*, *36*(2), 207–213. https://doi.org/10.2307/3588331

Bitsch, V. (2005). Qualitative research: A grounded theory example and evaluation criteria. *Journal of Agribusiness*, *23*(1), 75–91. https://doi.org/10.22004/ag.econ.59612

Boyce, C., & Neale, P. (2006). *Conducting in-depth interviews: A guide for designing and conducting in-depth interviews for evaluation input*. Pathfinder International

Branco, S. F., & Davis, M. (2020). The minority fellowship program: Promoting representation within counselor education and supervision. *Professional Counselor*, *10*(4), 603–614. https://doi.org/10.15241/sfb.10.4.603

Brentano, F. (1995). *Psychology from an empirical standpoint*, (In Linda L. McAlister). Routledge.

Brimblecombe, F. (2020). The public interest in deleted personal data? The right to be forgotten's freedom of expression exceptions examined through the lens of Article 10 Echr. *Journal of Internet Law*, *23*(10), 1–29.

Brinkmann, S., & Kvale, S. (2015). Introduction to interview research. *Interviews: Learning the craft of qualitative research interviewing* (3rd ed.). (pp. 3–26). Sage.

Broadhurst, R., & Chang, L. Y. (2013). Cybercrime in Asia: Trends and challenges. *Handbook of Asian criminology* (pp. 49–63). Springer.

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

Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J., & Neville, A. J. (2014). The use of triangulation in qualitative research. *Oncology Nursing Forum, 41*, 545–547. https://doi.org/10.1188/14.ONF.545-547

Chan, N. N., Ahrumugam, P., Scheithauer, H., Schultze-Krumbholz, A., & Ooi, P. B. (2020). A descriptive phenomenological study of students' and school counsellors' *lived experiences* of cyberbullying and bullying. *Computers & Education*, *146*, 103755. https://doi.org/10.1016/j.compedu.2019.103755

Chan, N. N., Walker, C., & Gleaves, A. (2015). An exploration of students' lived experiences of using smartphones in diverse learning contexts using a descriptive phenomenological approach. *Computers & Education*, *82*, 96–106. https://doi.org/10.1016/j.compedu.2014.11.001

Chandarman, R., & Van Niekerk, B. (2017). Students' cybersecurity awareness at a private tertiary educational institution. *African Journal of Information and Communication Technology*, *20*, 133–155. https://doi.org/10.23962/10539/23572

Charalambous, A., Papadopoulos, R., & Beadsmoore, A. (2008). Ricoeur's descriptive phenomenology: An implication for nursing research. *Scandinavian Journal of Caring Sciences*, *22*(4), 637–642. https://doi.org/10.1111/j.1471-6712.2007.00566.x

Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security, 30*, 719–731. https://doi.org/10.1016/j.cose.2011.08.004

Clandinin, D. J., & Connelly, F. M. (2000). From field to field texts: Being in a place of stories. *Narrative inquiry: Experience and story in qualitative research* (pp. 80–91). Josey-Bass.

Cole, J. I., Suman, M., Schramm, P., Zhou, L., & Salvador, L. (2013). *The digital future project 2013: Surveying the digital future*. Center for the Digital Future. Retrieved from https://www.digitalcenter.org/wp-content/uploads/2013/06/2013-Report.pdf

Cope, D. G. (2014). Methods and meanings: Credibility and trustworthiness of qualitative research. *Oncology Nursing Forum*, *41*(1), 89–91. https://doi.org/10.1188/14.ONF.89-91

Covell, C. L., Sidani, S., & Ritchie, J. A. (2012). Does the sequence of data collection influence participants' responses to closed and open-ended questions? A methodological study. *International Journal of Nursing Studies*, *49*, 664–671. https://doi.org/10.1016/j.ijnurstu.2011.12.002

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review, 4*, 13–21. Retrieved from https://timreview.ca/article/835

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32*, 90–101. https://doi.org/10.1016/j.cose.2012.09.010

Czarniawska, B. (2004). The narrative turn in social studies. *Narratives in social science research* (pp. 1–15). Sage.

Dawidowicz, P. (2016). Phenomenology. In G. J. Burkholder, K. A. Cox, & L. M. Crawford (Eds.), *The scholar-practitioner's guide to research design* (pp. 203–214). Laureate.

de la Torre, L. (2018). *A guide to the California Consumer Privacy Act of 2018.* https://doi.org/10.2139/ssrn.3275571

Denzin, N. K. (1970). *The research act: A theoretical introduction to sociological methods*. Aldine

Denzin, N. K., & Lincoln, Y. S. (2005). Introduction: The discipline and practice of qualitative research (pp. 1–42). *The Sage handbook of qualitative research* (3rd ed.). Sage.

DLA Piper Intelligence (2020). *Data protection laws of the world: Definition of personal data*. Retrieved from https://www.dlapiperdataprotection.com/index.html?t=definitions&c=US

Dlamini, M. T., Eloff, J. H., & Eloff, M. M. (2009). Information security: The moving target. *Computers & Security*, *28*, 189–198. https://doi.org/10.1016/j.cose.2008.11.007

Dowling, M. (2007). From Husserl to van Manen. A review of different phenomenological approaches. *International Journal of Nursing Studies*, *44*(1), 131–142. https://doi.org/10.1016/j.ijnurstu.2005.11.026

Ellis, C., & Bochner, A. (2000). Autoethnography, personal narrative, reflexivity: Researcher as subject. In N. Denzin & Y. Lincoln (Eds.). *The handbook of qualitative research* (2nd ed.). (pp. 733–768). Sage.

Engberg, K. (2013). The first operations. *The EU and military operations: A comparative analysis* (pp. 53–60). Routledge.

Errasti-Ibarrondo, B., Jordán, J. A., Díez-Del-Corral, M. P., & Arantzamendi, M. (2018). Conducting phenomenological research: Rationalizing the methods and rigor of the phenomenology of practice. *Journal of Advanced Nursing, 74*, 1723–1734. https://doi.org/10.1111/jan.13569

Fawaz, K., & Shin, K. G. (2019). Security and privacy in the Internet of Things. *Computer*, *52*(4), 40-49. https://doi.org/10.1109/MC.2018.2888765

Fetterman, D. M. (2010). *Ethnography: Step-by step* (3rd ed.). Sage.

Fochtman, D. (2008). Phenomenology in pediatric cancer nursing research. *Journal of Pediatric Oncology Nursing*, *25*(4), 185–192. https://doi.org/10.1177/1043454208319186

Furnell, S., Tsaganidi, V., & Phippen, A. (2008). Security beliefs and barriers for novice Internet users. *Computers & Security*, *27*, 235–240. https://doi.org/10.1016/j.cose.2008.01.001

Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report*, *20(9)*, 1408–1416. https://doi.org/10.46743/2160-3715/2015.2281

Gadamer, H. G. (1997). Truth and method. (2nd rev. ed.) (J. Weinsheimer and D. G. Marshall, Trans. rev.). New York, NY: Continuum. (Original work published 1960).

Galt, K. A., Fuji, K. T., Kaufman, T. K., & Shah, S. R. (2019). Health information technology use and patient safety: Study of pharmacists in Nebraska. *Pharmacy*, *7*(1), 7. https://doi.org/10.3390/pharmacy7010007

Giorgi, A. (2009). *The descriptive phenomenological method in psychology: A modified Husserlian approach*. Pittsburgh, PA: Duquesne University Press.

Glaser, B. G. (1999). The future of grounded theory. *Qualitative Health Research*, *9*, 836–845. https://doi.org/10.1177/104973299129122199

Glaser, B. G., & Strauss, A. L. (1967). *The discovery of grounded theory: Strategies for qualitative research.* Aldine.

Goduka, N. (2012). From positivism to indigenous science: A reflection on world views, paradigms, and philosophical assumptions. *Africa Insight, 41*, 123–138. Retrieved from https://scholar.google.com/scholar?hl=en&as_sdt=0%2C21&q=Goduka%2C+N.+%282012%29.+From+positivism+to+indigenous+science%3A+A+reflection+on+world+views%2C+paradigms%2C+and+philosophical+assumptions.+Africa+Insight%2C+41%2C+123%E2%80%93138.&btnG=

Goodall, Jr., H. L. (2000). *Writing the new ethnography*. AltaMira Press.

Guest, G., Bunce, A., & Johnson, L. (2006). How many interviews are enough? An experiment with data saturation and variability. *Field Methods, 18*(1), 59–82. https://doi.org/10.1177/1525822X05279903

Habermas, J. (1999). From Kant to Hegel and back again: The move towards detranscendentalization. *European Journal of Philosophy*, *7*, 129–157. Retrieved from https://msu.edu/~lotz/classes/f2006intersubjectivity/pdfs/habermas%20from%20kant%20to%20hegel.pdf

Hegel, G. W. F. (2018). *Georg Wilhelm Friedrich Hegel: The phenomenology of spirit*. Cambridge University Press.

Heidegger, E, M. (1962). *Being and time*. Harper.

Heidegger, M. (2010). *Phenomenological interpretations of Aristotle: Initiation into phenomenological research*. University Press

Hein, S. F., & Austin, W. J. (2001). Empirical and descriptive approaches to phenomenological research in psychology: A comparison. *Psychological Methods*, *6*(1), 3–17. https://doi.org/10.1037/1082-989X.6.1.3

Holt, A. (2010). Using the telephone for narrative interviewing: A research note. *Qualitative Research*, *10*(1), 113–121. https://doi.org/10.1177%2F1468794109348686

Houghton, C., Casey, D., Shaw, D., & Murphy, K. (2013). Rigor in qualitative case-study research. *Nurse Researcher*, *20*, 12–17. Retrieved from https://scholar.google.com/scholar?hl=en&as_sdt=0%2C21&q=Houghton+casey+shamurphy+2013&oq=Houghton%2C+Casey%2C+Shaw%2C

Hubick, J. (2018). Heretical Hindsight: Patočka's Phenomenology as questioning philosophy. *Journal of the British Society for Phenomenology*, *49*(1), 36–54. https://doi.org/10.1080/00071773.2017.1387685

Husserl, E. (1967). The thesis of the natural standpoint and its suspension. In J. Kockelmans (Ed.), *Phenomenology* (pp. 68–79). Doubleday.

Husserl, E. (1970). *The idea of phenomenology*. Nijhoff.

Husserl, E. (2012). *Ideas: General introduction to pure phenomenology*. Routledge.

International Telecommunication Union (2015). *The world in 2014: ICT facts and figures*. https://doi.org/10.1080/17482798.2014.961496

Jackson, C., Vaughan, D. R., & Brown, L. (2018). Discovering lived experiences through descriptive phenomenology. *International Journal of Contemporary Hospitality Management*. https://doi.org/10.1108/IJCHM-10-2017-0707

Jacob, S. A., & Furgerson, S. P. (2012). Writing interview protocols and conducting interviews: Tips for students new to the field of qualitative research. *The Qualitative Report*, *17*, 1–10. Retrieved from https://nsuworks.nova.edu/tqr/vol17/iss42/3

Jia, X., Wang, R., Liu, J. H., & Jiang, C. (2021). Discovery of behavioral patterns in online social commerce practice. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, e1433. https://doi.org/10.1002/widm.1433

Johansson, A., & Götestam, K. G. (2004). Internet addiction: Characteristics of a questionnaire and prevalence in Norwegian youth (12–18 years). *Scandinavian Journal of Psychology, 45*, 223–229. https://doi.org/10.1111/j.1467-9450.2004.00398.x

Johnston, A., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, 549–566. https://doi.org/10.2307/25750691

Kant, I. (1994). *Ethical philosophy* (2nd ed.). Hackett.

Karjalainen, M., & Siponen, M. (2011). Toward a new meta-theory for designing information systems (IS) security training approaches. *Journal of the Association for Information Systems*, *12*, 518. Retrieved from https://pdfs.semanticscholar.org/ab69/19eda04956523740099a8eea3fd781f0e8a9.pdf

Kazeroony, H. H. (2020). Phenomenology, perceptions, and methodology: An allegorical challenge. *Journal of the European Academy of Management*.

Kritzinger, E. (2017). Cultivating a cyber-safety culture among school learners in South Africa. *Africa Education Review*, *14*(1), 22–41. https://doi.org/10.1080/18146627.2016.1224561

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*, *25*, 289–296. https://doi.org/1016/j.cose.2006.02.008

Kruth, J. G. (2015). Five qualitative research approaches and their applications in parapsychology I. *The Journal of Parapsychology*, *79*, 219–233. Retrieved from https://search.proquest.com/openview/27127bb8d0ea9fad6d8f02ea3c382ad3/1?pq-origsite=gscholar&cbl=42308

Leech, N. L., & Onwuegbuzie, A. J. (2007). An array of qualitative data analysis tools: A call for data analysis triangulation. School Psychology Quarterly, 22(4), 557–584. https://doi.org/doi:10.1037/1045-3830.22.4.557

Leedy, P., & Ormrod, J. (2015). Qualitative research methods. *Practical research: Planning and design* (11th ed.), (pp. 269–295). Pearson Merrill Prentice Hall.

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. Sage.

Loibl, T. R. (2005, September). Identity theft, spyware and the law. In *Proceedings of the 2nd Annual Conference on Information Security Curriculum Development* (pp. 118–121). ACM. https://doi.org/10.1145/1107622.1107650

Magolis, D., & Briggs, (2016). A phenomenological investigation of social networking site privacy awareness through a media literacy lens. *Journal of Media Literacy Education*, *8*, 22–34. Retrieved from https://digitalcommons.uri.edu/cgi/viewcontent.cgi?article=1167&context=jmle

Matua, G. A., & Van Der Wal, D. M. (2015). Differentiating between descriptive and interpretive phenomenological research approaches. *Nurse Researcher*, *22*(6). https://doi.org/10.7748/nr.22.6.22.e1344

McConnell-Henry, T., Chapman, Y., & Francis, K. (2009). Husserl and Heidegger: Exploring the disparity. *International Journal of Nursing Practice*, *15*(1), 7–15. https://doi.org/10.1111/j.1440-172X.2008.01724.x

Merleau-Ponty, M. (1962). *Phenomenology of perception*. Routledge and Kegan Paul.

Merleau-Ponty, M. (1964). *The primacy of perception: And other essays on phenomenological psychology, the philosophy of art, history, and politics*. Evanston, IL: Northwestern University.

Moustakas, C. (1994). *Phenomenological research methods.* Sage.

Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and Organization*, *17*(1), 2–26. https://doi.org/10.1016/j.infoandorg.2006.11.001

NIST (2020). National Institute of Standards and Technology Special Publication 800–53, Revision 5 Natl. Inst. Stand. Technol. Spec. Publ. 800-53, Rev. 5, 492 pages. https://doi.org/10.6028/NIST.SP.800-53r5

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). http, 1–12. https://doi.org/10.1177%2F1609406917733847

Novick, G. (2008). Is there a bias against telephone interviews in qualitative research? *Research in Nursing & Health*, *31*, 391–398. Retrieved from https://onlinelibrary.wiley.com/doi/pdf/10.1002/nur.20259

O'Reilly, M., & Parker, N. (2012, May). Unsatisfactory saturation: A critical exploration of the notion of saturated sample sizes in qualitative research. *Qualitative Research Journal*, *13*(2), 1–8. https://doi.org/10.1177/1468794112446106

Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security*, *56*, 83–93. https://doi.org/10.1016/j.cose.2015.10.002

Oltmann, S. M. (2016). Qualitative interviews: A methodological discussion of the interviewer and respondent contexts. *Forum: Qualitative Social Research*, *17*, 1. https://doi.org/10.17169/fqs-17.2.2551

Onwuegbuzie, A. J., Leech, N. L., & Collins, K. M. (2012). Qualitative Analysis Techniques for the Review of the Literature. *The Qualitative Report*, *17*(28), 1–28. https://doi.org/10.46743/2160-3715/2012.1754

Opdenakker, R. (2006). Advantages and disadvantages of four interview techniques in qualitative research. *Qualitative Social Research, 7*, Article 11. https://doi.org/10.17169/fqs-7.4.175

Patton, M. Q. (2015). *Qualitative research and evaluation methods* (4th ed.). Sage.

Pizzolante, R., Castiglione, A., Carpentieri, B., De Santis, A., Palmieri, F., & Castiglione, A. (2018). On the protection of consumer genomic data in the Internet of Living Things. *Computers & Security*, *74*, 384–400. https://doi-org./10.1016/j.cose.2017.06.003

Polit, D., & Beck, C. (2012). Essentials of nursing research. *Ethics*, *23*. Retrieved from https://scholar.google.com/scholar?hl=en&as_sdt=0%2C21&q=Polit+%26+Beck%2C012&oq=po

Pope, C., Ziebland, S., & Mays, N. (2000). Analysing qualitative data. *The BMJ*, *320*(7227), 114–116. https://doi.org/10.1136/bmj.320.7227.114

Posey, C., Roberts, T. L., Lowry, P. B., & Hightower, R. T. (2014). Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information & Management*, *51*, 551–567. https://doi.org/10.2139/ssrn.2418233

Purtova, N. (2018). The law of everything: Broad concept of personal data and future of EU data protection law. *Law, Innovation & Technology*, *10*(1), 40–81. https://doi.org/10.1080/17579961.2018.1452176

Qutoshi, S. B. (2018). Phenomenology: A philosophy and method of inquiry. *Journal of Education and Educational Development*, *5*(1), 215–222. Retrieved from https://www.journals.iobmresearch.com/index.php/JoEED/article/view/2154

Rahim, N. H. A., Hamid, S., Mat Kiah, M. L., Shamshirband, S., & Furnell, S. (2015). A systematic review of approaches to assessing cybersecurity awareness. *Kybernetes*, *44*, 606–622. https://doi.org/10.1108/K-12-2014-0283

Rahim, N. H. A., Hamid, S., & Kiah, L. M. (2019). Enhancement of cybersecurity awareness program on personal data protection among youngsters in Malaysia: An assessment. *Malaysian Journal of Computer Science*, *32*(3). https://doi.org/10.22452/mjcs.vol32no3.4

Rainie, L., Kiesler, S., Kang, R., Madden, M., Duggan, M., Brown, S., & Dabbish, L. (2013). Anonymity, privacy, and security online. *Pew Research Center*, *5*. Retrieved from https://www.pewinternet.org/wpcontent/uploads/sites/9/media/Files/Reports/2013/PIP_AnonymityOnline_090513.pdf

Rich, S., Graham, M., Taket, A., & Shelley, J. (2013). Navigating the terrain of lived experience: The value of lifeworld existentials for reflective analysis. *International Journal of Qualitative Methods*, *12*(1), 498–510. https://doi.org/10.1177/160940691301200125

Ricoeur, P. (2016). Architecture and narrativity. *Études Ricoeuriennes/Ricoeur Studies*, *7*(2), 31–42. https://doi.org/10.5195/errs.2016.378

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

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude: A revised theory of protection motivation. In J. Cacioppo & R. Petty (Eds.). *Social Psychophysiology*. Guilford.

Rubin, H. J., & Rubin, I. S. (2012). Data analysis in the responsive interview model. *Qualitative interviewing: The art of hearing data* (3rd ed.) (pp. 169–212). Sage.

Ruiz, R. (2015, April 8). F.C.C. fines AT&T $25 million for privacy breach. *The New York Times*. Retrieved from http://bits.blogs.nytimes.com/2015/04/08/f-c-c-fines-att25-million-for-privacy-breach/?ref=topics

Saldaña, J. (2016). An introduction to codes and coding. *The coding manual for qualitative researchers* (3rd ed.), (pp. 1–42). Sage.

Salvador, J. T. (2016). Exploring quantitative and qualitative methodologies: A guide to novice nursing researchers. *European Scientific Journal*, *12*. https://doi.org/10.19044/esj.2016.v12n18p107

Sanchez Alcon, J. A., Lopez, L., Martinez, J.-F., & Castillejo, P. (2013). Automated determination of security services to ensure personal data protection in the Internet of Things applications. *Third International Conference on Innovative Computing Technology (INTECH 2013),* 71–76. https://doi.org./10.1109/INTECH.2013.6653704

Schwandt, T. A., Lincoln, Y. S. & Guba, E. G. (2007). Judging interpretations: But is it rigorous? Trustworthiness and authenticity in naturalistic evaluation. *New Directions for Evaluation*, *207,* 11–25. https://doi.org/10.1002/ev.223

Shamsi, J. A., Zeadally, S., & Nasir, Z. (2016). Interventions in cyberspace: Status and trends. *IT Professional*, *18*(1), 18–25. https://doi.org/10.1109/MITP.2016.19

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H. J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, *52*(1), 92–100. https://doi.org/10.1016/j.compedu.2008.06.011

Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. *Education for information*, *22*, 63–75. https://doi.org/10.3233/EFI-2004-22201

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

Silverman, H. (Ed.). (1991). Gadamer and descriptives. Routledge. https://doi.org/10.4324/9781315543024

Singer, P. W., & Friedman, A. (2014). How it all works. *Cybersecurity and cyberwar: What everyone needs to know* (pp. 12–64). OUP.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8*(1), 31–41. https://doi.org/10.1108/09685220010371394

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, *51*, 217–224. https://doi.org/10.1016/j.im.2013.08.006

Sithira, V., & Nguwi, Y. Y. (2014). A study on the adolescent online security issues. *International Journal of Multidisciplinary Research*, *2*, 596–601. Retrieved from http://ijmcr.com/wp-content/uploads/2014/06/Paper14596-601.pdf

Slattery, P., Krasny, K. A., & O'Malley, M. P. (2007). Descriptives, aesthetics, and the quest for answerability: A dialogic possibility for reconceptualizing the interpretive process in curriculum studies. *Journal of Curriculum Studies*, *39*(5), 537–558. https://doi.org/10.1080/00220270600911039

Thurmond, V. A. (2001). The point of triangulation. *Journal of Nursing Scholarship*, *33*(3), 253–258. Retrieved from https://msessd.ioe.edu.np/wp-content/uploads/2017/04/the-point-of-triangulation.pdf

Tsai, H. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, *59*, 138–150. https://doi.org/10.1016/j.cose.2016.02.009kk

Twisdale, J. A. (2018). *Exploring SME vulnerabilities to cyber-criminal activities through employee behavior and Internet access*. (Doctoral dissertation, Walden University).

U.S. Department of Justice. (2011). *Identity theft and identity fraud*. Retrieved from http://www.justice.gov/criminal/fraud/websites/idtheft.html

United States Cyberspace Policy Review (The) (2009). Retrieved from https://fas.org/irp/eprint/cyber-review.pdf

Valle, R. S., King, M., & Halling, S. (1989). An introduction to existential-phenomenological thought in psychology. In R. S. Valle and S. Halling (Eds.), *Existential-phenomenological perspectives in psychology. Exploring the breadth of human experience* (pp. 3–16). Springer.

van Manen, M. (1984). Practicing phenomenological writing. *Phenomenology+ Pedagogy*, 36–69. Retrieved from https://journals.library.ualberta.ca/pandp/index.php/pandp/article/view/14931/11752

van Manen, M. (2002). *Writing in the dark: Phenomenological studies in interpretive inquiry*, 237–253. The Althouse Press.

van Manen, M. (2014). *Phenomenology of practice: Meaning-giving methods in phenomenological research and writing*. Left Coast Press.

van Manen, M. (2015). *Researching lived experience: Human science for an action sensitive pedagogy* (2nd ed.). Left Coast Press.

Vogl, S. (2013). Telephone versus face-to-face interviews: Mode effect on semi-structured interviews with children. *Sociological Methodology, 43*(1), 133–177. https://doi.org/10.1177%2F0081175012465967

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*(0), 97–102. https://doi.org/10.1016/j.cose.2013.04

Wang, K., & Sarkar, S. (2019). *Nudging young people towards safe Internet behavior*. Retrieved from https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1425&context=amcis2019

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems*, *18*, 101–105. https://doi.org/10.1057/ejis.2009.12

Wertz, F. J. (2010). [Review of the book: The descriptive phenomenological method in psychology: A modified Husserlian approach, by A. Giorgi]. Journal of Phenomenological Psychology, 41(2), 269–276. https://doi.org/10.1163/156916210X526079

Willig, C. (2013). Qualitative research design. *Introducing qualitative research in psychology: Adventures in theory and method* (pp. 15–30). McGraw-Hill.

Wolcott, H. F. (2016). Minding the ethnographic lesson. *Ethnography lessons: A primer* (pp. 33–43). Routledge.

Yin, R., K. (2014). Getting started. *Case study research: Design and methods* (5th ed.), (pp. 1–28). Sage.

Zadvinskis, I. M., Smith, J. G., & Yen, P. Y. (2018). Nurses' experience with health information technology: Longitudinal qualitative study. *JMIR Medical Informatics*, *6*, e38. https://doi.org/10.2196/medinform.8734

Zhang, P., Durresi, M., & Durresi, A. (2019). Multi-access edge computing aided mobility for privacy protection in Internet of Things. *Computing*, *101*(7), 729–742. https://doi.org/10.1007/s00607-018-0639-0

Appendix A: Protecting Human Research Participants Certificate of Completion

Certificate of Completion

The National Institutes of Health (NIH) Office of Extramural Research certifies that **Emmanuel Segun** successfully completed the NIH Web-based training course “Protecting Human Research Participants”.

Date of completion: 09/27/2011

Certification Number: 753705

Appendix B: Interview Protocol

Interview Title: Exploration of Cybersecurity Managers' Experiences Protecting Users' Privacy

1. How have you navigated the adoption of new data security laws to protect users' privacy?

2. How would you describe the Internet of Things (IoT)? Please elaborate.

   How have you navigated the adoption of the IoT to protect users' privacy?

3. How has the enablement of new applications by IoT affected the protection of users' privacy?

4. How would you describe your experiences in providing protection of individual's personal data in cyberspace services? Please explain.

5. How do you go about protecting data based on various regulations, and often contradictory legislations in various countries?

6. How has the protection of individual's personal data translated into the protection of individual's privacy in cyberspace?

7. How has the interactions among interconnected devices introduced more challenges for you as a cybersecurity or information security manager in protecting users' data and privacy in cyberspace?

8. Can you help me understand the differences of securing cloud-based and on-premises data protection?

   How could these hosting types affect the protection of users' data and privacy in cyberspace?

9. What is your understanding of a zero-day attack aka zero-day vulnerability?

   How could this attack affect the protection of users' data and privacy in cyberspace?

10. Finally, based on your experiences, how do you think cybersecurity awareness, privacy and personal data protection education can be provided to individual Internet users? Please explain.

Appendix C: Participant Invitation

Seeking cybersecurity managers in the Maryland, Washington DC, and Northern Virginia metro areas of the United States for a 30–60-minute phone/Zoom interview in the next 2 weeks, $10 gift card.

There is a new study called *"Exploration of Cybersecurity Managers' Experiences Protecting Users' Privacy"* that could help cybersecurity managers better understand how to protect users' data and privacy in cyberspace. For this study, you are invited to describe your lived experiences on how you have navigated the adoption of new data security laws, new applications, and the Internet of Things (IoT) to protect users' privacy in cyberspace.

This research is part of the doctoral study for Emmanuel Segun, a Ph.D. student at Walden University.

About the study:

- One 30-60-minute telephone or Zoom video interview.

Volunteers must meet these requirements:

- 18 years old or older
- With a minimum of 5 years' experience as a cybersecurity manager.

To confidentially volunteer, please, email me at:
Email address removed before publication.
Thank you very much.