2022

Exploring Security Strategies to Protect Personally Identifiable Information in Small Businesses

Erin Banks
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Erin Banks

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. Constance Blanson, Committee Chairperson, Information Technology Faculty
Dr. Okey Igbonagwam, Committee Member, Information Technology Faculty
Dr. Jon McKeeby, University Reviewer, Information Technology Faculty

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

Walden University
April 2022

Abstract

Exploring Security Strategies to Protect Personally Identifiable Information in Small Businesses

by

Erin H. Banks

MS, Walden University, 2016

MS, University of Maryland University College, 2014

BS, Excelsior College, 2004

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

April 2022

Abstract

Organizations that do not adequately protect sensitive data are at high risk of data breaches. Organization leaders must protect confidential information as failing to do so could result in irreparable reputation damage, severe financial implications, and legal consequences. This study used a multiple case study design to explore small businesses' strategies for protecting their customers' PII against phishing attacks. This study's population comprised information technology (IT) managers in small businesses in Northern Virginia. The conceptual framework used in this study was the technology acceptance model. Data collection was performed using telephone interviews with IT managers (*n* = 6) as well as secondary data analysis of documents related to information security (*n* = 13). Thematic analysis was used to analyze and code the data, which resulted in four themes. The first theme to emerge was that users are the first line of defense in protecting PII. The second theme to emerge was that preventing phishing attacks is challenging for small businesses. The third theme to emerge was that users are a challenge in protecting PII from phishing attacks. The final theme to emerge was that user awareness and training is the best defense against phishing attacks. A recommendation is that information security training should be performed consistently while senior leadership fosters an environment that promotes acceptable security behavior and attitudes. The findings of this study may promote positive social change by helping IT leaders develop effective strategies or frameworks for protecting their customers' PII from phishing attacks.

Exploring Security Strategies to Protect Personally Identifiable Information in Small Businesses

by

Erin H. Banks

MS, Walden University, 2016

MS, University of Maryland University College, 2014

BS, Excelsior College, 2004

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

April 2022

Dedication

I would like to dedicate this study to my family and friends. My husband and best friend, James Banks, your unwavering support, and confidence in me helped me achieve the title Dr. You are my number one cheerleader, and I am eternally grateful. My parents, William, and Helen Holley, instilled in me to not give up when the going gets tough. My sister, Kelly Holley-Poole, offered her editing and research skills to help me complete this study. Thank you for everything. My good friend, Jonathan Butler, lent me his ear throughout this journey and refused to let me throw in the towel. I am fortunate to have you as a friend. My cousins-in-law Dr. Sonya Brown and Dr. Tyrana Battle, you motivated and inspired me to start this journey. You are my sheroes.

Acknowledgments

First, I would like to thank my committee chair, Dr. Constance Blanson, for her guidance, mentorship, and support during my doctoral journey. I can hardly believe that we finally made it to this point. Her calm demeanor and humor helped smooth the ride of a bumpy doctoral journey. Second, I would like to thank my second committee members, Dr. Richmond Adebiaye and Dr. Okey Igbonagwam. Their valuable comments and feedback were vital for the completion of my doctoral study. Lastly, I would like to thank all the participants in my study for sharing their time and experiences with me.

Table of Contents

List of Tables

Section 1: Foundation of the Study

Government agencies and corporations rely on small businesses to provide the goods and services required to sustain their operations. These organizations often share personally identifiable information (PII) with small businesses to support business operations. However, due to a lack of expertise, funding, and effective policies, small businesses find it increasingly difficult to secure their customers' PII from phishing attacks. The inability to protect customers' PII from phishing attacks places some small businesses at risk of devastating reputation damage and financial repercussions.

Background of the Problem

Customers expect businesses to protect their customers' PII; however, some small businesses lack strategies to protect their customers' PII from phishing attacks. Limited budgets and expertise often prevent some small businesses from implementing strategies designed to protect their customers' PII from phishing attacks (Small Business Administration [SBA], 2019). Cybercriminals target small businesses due to their perceived inability to protect their customers' PII from phishing attacks adequately. Effective information security management systems can help small businesses avoid the consequences of PII breaches (Ionescu et al., 2018).

Problem Statement

Small businesses are vulnerable to phishing attacks resulting in PII data breaches because of limited security resources (Harris, 2016). Small businesses account for approximately 72% of data breaches (Fielder et al., 2016), with research demonstrating that 80% of small businesses were unaware of their legal or regulatory obligation to protect PII (Watad et al., 2018). The general IT problem is that preventing phishing attacks resulting in PII data breaches because of limited security resources is challenging for some small businesses. The specific IT problem is that small businesses' IT managers lack strategies for preventing phishing attacks resulting in PII data breaches.

Purpose Statement

The purpose of this qualitative multiple case study was to explore strategies used by IT managers in small businesses to protect customers' PII from phishing attacks. The sample population consisted of IT managers responsible for securing small businesses' networks. The location of this study was Alexandria, Virginia, in the United States. Small business leaders may find this study helpful in identifying strategies that can help protect their customers' PII against phishing attacks. This study may promote positive social change because it provides strategies for small businesses to safeguard their data and information against theft or intrusions.

Nature of the Study

I chose a qualitative methodology for this study. Qualitative research was appropriate for this study because it requires participants to describe experiences in explicit detail. Qualitative research is suitable for asking "how" or "why" questions (Tai & Ajjawi, 2016). I conducted semistructured interviews and asked interviewees open-ended questions to collect in-depth descriptions of strategies used to protect their customers' PII against phishing attacks. A quantitative research methodology was not suitable for this study because quantitative research aims for replicability under controlled conditions (Park & Park, 2016).

Mixed-method approaches combine qualitative and quantitative methods. Research problems that require multiple methodologies for in-depth exploration are suited for a mixed-method design (Doyle et al., 2009). With mixed-method designs, research is complete when data saturation occurs qualitatively and quantitatively. Due to the time and resource-intensive nature of this method, it was not appropriate for this study.

I evaluated several designs and chose to use a multiple case study design. Case study researchers explore a phenomenon within specific boundaries to investigate research questions (Alpi & Evans, 2019). The limits to analyze the information security strategies used by small businesses were the boundaries of the three cases selected to participate in this study. Phenomenological researchers seek to understand what an event, place, or thing means to a group or individuals who lived through the phenomenon (Alpi & Evans, 2019). The purpose of this study was to identify the strategies that small businesses use to protect their customers' PII against phishing attacks; therefore, a phenomenological design was not appropriate for this study. Ethnography researchers explore a phenomenon based on the shared experience of members of a culture or society over time (Hayes et al., 2015). I did not seek to engage with study participants over an extended period; thus, an ethnographical design was inappropriate for this study.

Research Question

How do small businesses protect their customers' PII against phishing attacks?

Interview Questions

- What types of phishing attacks against customers' PII has your business experienced?
- How do you protect your customers' PII against phishing attacks?
- What are the considerations involved when developing strategies for protecting your customers' PII against phishing attacks?
- What techniques have you found most effective in protecting your customers' PII against phishing attacks?
- What are the challenges relative to the strategies used in protecting your customers' PII against phishing attacks?
- What types of training are offered to customers to protect their PII against phishing attacks?
- What additional information about your experiences protecting your customers' PII against phishing attacks would you like to share?

Conceptual Framework

This study's conceptual framework was the technology acceptance model (TAM) developed by Davis in 1986. TAM evolved from the theory of reasoned action (TRA) (Shih, 2004). Proponents of TAM aim to explain and predict the conditions under which users accept and adopt information technology at the individual level (Ajibade, 2018; Ritz et al., 2019). TAM consists of two constructs: perceived usefulness (PU) and perceived ease of use (PEOU). PU refers to an individual's belief that a particular computing system will improve their job performance (Davis, 1989). PEOU refers to the user’s belief that specific computing technologies are simple to learn and use (Davis, 1989). In the context of protecting PII, PU refers to the degree to which small business leaders believe that employing security measures to protect PII will help them avoid the consequences of compromised PII. PEOU refers to the simplicity of implementing security strategies to protect PII. TAM relates to the influences that motivate a person to use a specific innovative technology. The primary goal of TAM is to analyze the impact of external factors on users’ internal thoughts, feelings, and intentions to adopt a specific system (Davis et al., 1989). Researchers have used TAM to study users’ acceptance of technologies associated with mobile learning, digital libraries, gamification, and social media (Sprenger & Schwaninger, 2021).

I sought to connect the TAM elements PU and PEOU in IT managers’ acceptance of PII protection strategies. PU refers to the usefulness of policies and technologies in their ability to safeguard PII. PEOU relates to the ease with which IT managers can create, implement, and maintain policies and technologies that protect PII. TAM aligned well with this study, as IT managers are likely to support implementing policies and technologies to protect PII if they perform well and are and simple to use.

Supporting Theory

The Unified Theory of Acceptance and Use of Technology (UTAUT)

The unified theory of acceptance and use of technology (UTAUT) was developed by Venkatesh et al. in 2003 (Davis, 1986; Venkatesh et al., 2003). UTAUT, an extension of TAM, seeks to explain and predict user acceptance and adoption of technology in organizations (Reyes-Mercado & Barajas-Portas, 2020). UTAUT consists of four factors:

social influence (SI), effort expectancy (EE), facilitating conditions (FC), and performance expectancy (PE; Gunawan et al., 2019). SI refers to how others perceive the new system regarding the benefits associated with its usage (Puriwat & Tripopsakul, 2021). EE refers to the ease of use of the system (Puriwat & Tripopsakul, 2021). FC refer to how a user believes that technical and organizational infrastructure supports system usage (Puriwat & Tripopsakul, 2021). The expectancy of performance refers to the extent to which users believe that a system will help them perform their jobs (Puriwat & Tripopsakul, 2021). Researchers have applied UTAUT to studies concerning social media, e-commerce, and digital advertising platforms (Puriwat & Tripopsakul, 2021; Reyes-Mercado & Barajas-Portas, 2020; Susanty et al., 2020).

I evaluated the circumstances that result in the lack of acceptance or adoption of PII protection strategies in small businesses using the UTAUT behavioral factors EE, PE, and SI. EE relates to the effort needed to develop, implement, and maintain PII policies, processes, and technologies. PE refers to the performance requirements of PII protection strategies implemented by IT managers. Social influences from internal and external sources contribute to IT managers' behavioral intentions to accept or reject PII protection processes and technologies. UTAUT aligned well with this study as successful PII security strategies require implementing technology that is easy to use, performs as expected, has straightforward security policies, and involves user security education that applies to the current threat environment and the intended audience.

Contrasting Theories

Grey systems theory is a contrasting theory relative to GST. Deng Julong developed grey systems theory in 1982 (Liu et al., 2017). *Grey systems* are systems in which there is partial and incomplete knowledge of the system or phenomena (Lin, 2017; Mierzwiak et al., 2019). Razaque et al. (2020) contended that standard statistical methods are too restrictive to handle the uncertainties associated with grey systems. Razaque et al. also argued that it is possible to identify qualitative and quantitative relationships between complex elements with limited information using a grey systems methodology. Grey systems theory is suitable for generating forecasting models for decision making (Mierzwiak et al., 2019). Researchers have applied grey systems theory to study issues that impact information and communication technology (ICT). Soni et al. (2017) examined the efficacy of e-governance, focusing on grey areas of ICT such as information security breaches and IT policy implementation. Soni et al. suggested that the flexible multicriteria decision-making (MCDM) element of grey systems theory helped them establish a path forward for the grey sectors of ICT. The main point to argue is that grey systems consist of anonymous information. The researcher must fill in the knowledge gaps with fuzzy details to create a predictive model for decision making. In my research, I aimed not to make any decisions or help the participants make decisions; I wanted to find out what they were doing to secure their information and prevent data breaches.

Definition of Terms

Cybersecurity: This security mode features preventive measures designed to protect data from attack, loss, theft, or compromise (Billingsley, 2019).

Information security: The preservation of the confidentiality, integrity, and availability of information, including the information systems and networks used to process, store, and transmit data (McLaughlin & Gogan, 2018).

Information security manager: Staff member responsible for developing organizational strategies and procedures to protect information assets (Hasbini et al., 2018).

Small business: An organization with less than 500 employees (SBA, 2019).

Personally identifiable information (PII): Any information that can identify a specific individual (Paulsen & Toth, 2016).

Assumptions, Limitations, and Delimitations

Assumptions

I made two assumptions during research for this study. Assumptions are ideas, theories, or frameworks considered factual or truthful without definitive evidence (Waldkirch, 2020). The first assumption was that interview questions would produce rich, thick data to address the research question. The second assumption was that participants would provide honest, candid responses to questions posed during semistructured interviews. Although there was no way to definitively assure that the content of participants' speech accurately reflected the thoughts in their minds, for this study, it was assumed that the responses that participants gave were honest. To ensure that this was the case, I made sure that participants knew that their responses would be anonymous and that there were no risks in this study that might jeopardize their personal, professional, or financial well-being.

Limitations

In qualitative research, restrictions beyond the researcher’s control, such as small sample size and time constraints, are considered limitations (Theofanidis & Fountouki, 2018). One limitation of this study was that the results may not be generalizable to the small business population. Another limitation was using sampling for data collection because I could not interview all IT managers in small businesses. A third limitation was my role as an instrument. It was possible that I would misinterpret the data according to my own biases or a misunderstanding of participants’ responses. In this study, I took the steps outlined in this chapter to reduce researcher limitations in qualitative research.

Delimitations

Delimitations are boundaries that help the researcher scope the study for manageability or fill knowledge gaps (Alpi & Evans, 2019). The researcher’s self-imposed restrictions concerning theoretical lenses, research questions, and sample size are delimitations in qualitative research (Theofanidis & Fountouki, 2018). The first delimitation was that the study consisted of IT managers of small businesses with at least 3 years of experience. The second delimitation was the geographic location of the study, which was limited to Alexandria, Virginia.

Significance of the Study

Contribution to Information Technology Practice

IT managers in small businesses are responsible for implementing strategies designed to protect their customers' PII against phishing attacks. This study is significant because it may provide IT managers with effective strategies or frameworks for protecting their customers' PII from phishing attacks. Stable, successful small businesses contribute to the global economy by creating jobs, engaging in innovation, delivering goods and services, and providing tax revenue. Through improved strategies to protect customers' PII, small businesses may avoid the consequences of having their customers' PII compromised.

Implications for Social Change

Implications for positive social change include adding to the body of knowledge of strategies for IT managers and organizations to protect customers' PII against phishing attacks. The lessons learned can also be shared at home. There is also the potential to contribute new insights that may help in developing new strategies for small businesses to safeguard their data and information against theft or intrusions.

A Review of the Professional and Academic Literature

Overview

The purpose of this qualitative multiple-case study was to explore strategies used by small businesses to protect their customers' PII against phishing attacks. The literature review consisted of 100 articles from journals, papers, dissertations, reports, and seminal books, focusing on research conducted within the past 5 years. I used the Walden

University Library to access databases to gather analysis. The databases included were Science Direct, Sage, EBSCO, ProQuest, Google Scholar, Emerald Insight, Taylor & Francis Online, and the Computer Science database. While searching, the terms used included *small business*, *SME and cybersecurity*, *data breaches*, *information security*, and *data security.*

I cite 85 peer-reviewed articles in this literature review. I verified that articles were peer reviewed through Ulrich Periodicals Database or by going to the journal website for verification. I explain the conceptual frameworks, the TAM and UTAUT. I also provide a general background on TAM, its variables, and UTAUT. Additionally, I discuss contrasting and supporting theories within the conceptual framework section and related studies that have used TAM and UTAUT and discuss applying the literature to the applied IT problem at the heart of the research project. Several strategies to protect data are revealed, including technical and physical preventative measures and awareness strategies.

Conceptual Frameworks

Technology Acceptance Model (TAM)

Several information security researchers have examined information security using TAM. Davis (1989) developed TAM to offer a general explanation for the influences that motivate users to adopt new technologies. TAM originated from the theory of reasoned action (TRA) and the theory of planned behavior (TPB; Fishbein & Ajzen, 1977; Ritz et al., 2019). The goal of TRA is to explain how a person's thoughts and feelings influence their intention to engage in a particular behavior (Mohamad et al., 2021). Ajzen's (1991) TPB expands TRA by considering an individual as having perceived behavioral control, attitude towards conduct, and subjective norms for predicting their intent to engage in a specific behavior. TAM goes further by combining both theories and adding PU and PEOU to explain the behavioral aspects of users' technology usage intentions. In the context of this study, PU refers to the level at which an IT manager believes that implementing new technology could improve their ability to protect PII from phishing attacks. PEOU refers to the degree to which an information security professional believes that an information security system will be easy to learn and simple to use.

TAM provides researchers in the information security and IT fields a framework for determining the probability of users' acceptance and usage of new technology (Zabukovšek et al., 2019). User feedback regarding the PU and PEOU of a system can help system designers create a valuable and accepted product. Researchers have applied the TAM to various technologies and user populations, including cloud computing, education, business, and banking (Bayraktaroglu et al., 2019). Sengkhyavong (2019), Pereira (2020), and Pruitt (2019) applied TAM to identify the factors related to IT managers' decision to adopt cloud computing. Sengkhyavong found that PEOU, PU, and perceived benefits of cloud computing were significant factors in IT managers' decisions to adopt cloud computing. Pereira discovered a significant positive relationship between PU, security, regulatory environment, and IT managers' choice to adopt cloud computing. At the same time, Pruitt saw that authentication security, data protection security, physical security, PU, and PEOU influenced IT managers to adopt cloud computing. Sondakh (2017) applied the TAM to predict taxpayers' interest in using electronic tax returns and found that PEOU had a significant positive effect on PU and users' attitudes toward electronic tax services. Ramadania and Braridwan (2019) applied the TAM to measure the influence of PU, PEOU, attitude, self-efficacy attitude, and subjective norms towards users' intention to use online shopping. Ramadania and Braridwan found that users' PU, PEOU, attitude, self-efficacy, attitude, and subjective norms are directly proportional to the level of intent to use online shopping. The results of these studies align with Razmak and Bélanger's (2018) assertion that if users develop a positive relationship with an information system, they are more likely to use it.

Unified Theory of Acceptance and Use of Technology (UTAUT)

The UTAUT is an extension of TAM. While TAM measures user acceptance of technology at the individual level, UTAUT helps explain users' technology acceptance in an organizational context (Ajibade, 2018; Mohammad-Salehi et al., 2021). UTAUT combines eight conceptual models commonly used to describe the individual acceptance of technology (Venkatesh et al., 2003). The eight conceptual models are the TRA, the TAM, the motivational model (MM), the TPB, the model of PC utilization (MPCU), the innovation diffusion theory (IDT), and the social cognitive theory (SCT; Venkatesh et al., 2003). UTAUT consists of four components: EE, PE, SI, and FC (Puriwat & Tripopsakul, 2021). SI refers to how other IT managers view the usefulness of the new technology. In the context of this study, EE describes the system's ease of use. FC refers to IT managers' belief that appropriate support infrastructure exists for the new system. PE refers to how IT managers believe that new technology will help improve their job performance.

UTAUT offers researchers a framework for investigating the implementation of new IT systems at an institutional level (Garone et al., 2019). UTAUT addresses TAM's 40% variation in predicting users' intention to use technology (Mohammad-Salehi et al., 2021). According to Bu et al. (2021), UTAUT explains 70% of the variation in predicting users' intention to accept and use new information systems and technologies. Researchers have applied UTAUT to studies concerning social media, e-commerce, and digital advertising platforms (Puriwat & Tripopsakul, 2021; Reyes-Mercado & Barajas-Portas, 2020; Susanty et al., 2020). Puriwat and Tripopsakul (2021) applied UTAUT to their investigation of social media adoption in small businesses. Puriwat and Tripopsakul discovered that SI, effort, and PE greatly influenced the behavioral inclination to implement social media for business purposes. These findings align with those of Rozmi et al. (2019). Rozmi et al. investigated the intention of owners of small and medium-sized enterprises (SMEs) to adopt information and communication technology (ICT) and found that EE, SI, and FC influenced SME owners' intention to adopt ICT. The results of these studies support Varma's (2018) assertion that EE, PE, and SI are motivating factors in entrepreneur's decisions to adopt innovative technologies.

Applicability of the Technology Acceptance Model to the Study

Implementing an information security program is based on IT managers' and users' willingness to accept and adopt technologies and policies to protect data. Davis's (1986) TAM offers a general explanation for the influences that motivate users to adopt new technologies. Budgetary constraints and user expertise are examples of individual results, while organizational and legal standards represent environmental effects. Furthermore, information security policies must balance business requirements with ecological considerations, such as laws and industry regulations, to secure information and avoid data breaches. TAM aligned well with this study because small business IT managers judge the PEOU and PU of implementing strategies for protecting data, which aligns with the causal processes in the TAM.

Extensions of TAM

TAM is not without limitations. Davis (1989) acknowledged that PU and PEOU might not be the only intermediaries between attitude and system acceptance and adoption. Davis (1989) also wrote that TAM is a foundational model that future researchers can build upon and extend to explore a wide range of phenomena. Ajibade (2018) agreed that TAM has limitations. Ajibade argued that TAM is appropriate for describing individual acceptance and use of technology, but not explaining the reasons for accepting and using technology in a business environment. Ajibade introduced the technology acceptance and use model (TAUM) to explain IT adoption and use by small and medium-sized businesses. Ajibade’s TAUM involved consideration of organizational standards and guidelines with the type of tasks performed to advocate using a system.

To overcome the limitations of TAM, many researchers extended TAM to include a vast range of internal and external variables that apply to various technologies and contexts. Mushi (2018) used an extended TAM to investigate the impact of personal privacy on the acceptance of mobile phone technology in small and medium-sized enterprises. Mushi added personal privacy to TAM to determine the impact that personal privacy had on SMEs' acceptance and usage of mobile phones. Mushi found that personal privacy affected the PU of mobile phones, but it did not influence the behavioral intention to use them. When employees felt that their privacy was safe, they were more inclined to use mobile phones. Saroia and Gao (2019) also used an extended TAM to examine college students' intention to use mobile learning management systems (m-LMS). Saroia and Gao extended TAM to include academic relevance (AR), perceived mobility value (PMV), and university management support (UMS) as external variables to the adoption of m-LMS. PMV represents the students' judgment regarding the advantage of using m-LMS. AR refers to students' PU judgments regarding the relevance of m-LMS for their studies. UMS refers to the school's commitment to ensuring that the m-LMS operates as intended. Saroia and Gao found that UMS exhibited a strong relationship with PEOU. At the same time, PEOU directly influenced attitude towards usage.

Zain et al. (2019) contended that TAM's various external factors play a role in a system's PU and PEOU. Zain et al. extended TAM to include the external factors content quality (CQ) and motivation (Mo) to explore the factors influencing students' acceptance and usage of a web-based social media application. CQ refers to the degree to which students can use learning content within the application to improve academically. Zain et al. found that high CQ was a reliable predictor of students' PU and PEOU. This result aligns with Razmak and Bélanger's (2018) study that showed that the ability of a system to address users' needs is related to PU. Razmak and Bélanger also extended TAM to study the acceptance of electronic personal health records (PHR). Razmak and Bélanger expanded TAM to include compatibility and communicativeness to consider variations in users' behaviors and needs when using new technology.

Additionally, Castiblanco Jimenez et al. (2021) discovered that PU and PEOU are affected by the external TAM variables computer self-efficacy, individual innovativeness, computer anxiety, perceived enjoyment, social norm, content, and system quality experience and facilitating conditions. Results from Castiblanco Jimenez et al.'s study of external TAM variables in e-learning and virtual reality applications revealed that external variables affect PU and PEOU differently. The authors also found that self-efficacy was the strongest predictor of PEOU with experience and perceived enjoyment as secondary influences. At the same time, PEOU had a significant impact on PU and sensed pleasure, system, and content quality. Wang et al. (2020) also considered personal innovativeness in exploring consumers' intention to use ridesharing services. Wang et al. extended TAM to include external variables such as personal innovativeness (PI), environmental awareness (EA), and perceived risk (PR). Wang et al. found that PU, value, and convenience were the main motivations to use ridesharing.

All in all, both internal and external factors contribute to users' PU and PEOU of new technology. The relationships between these variables change depending on the technology and environment to which they are applied. Although TAM is famous in the information security and technology fields, researchers have extended and will continue to expand it to apply to a broad range of technologies and industries.

TAM was appropriate for this study because it evaluates the influences that motivate an IT manager to accept or reject security systems that protect PII. IT managers can use the TAM model to improve information security adoption in small businesses. Understanding the principles of the TAM is crucial in exploring the strategies that some small business IT managers use to protect PII. To better understand IT managers' acceptance of information security systems and policies, I examined several conceptual and theoretical models. However, I used the TAM as the conceptual framework because IT managers can apply the constructs behind users' behavior in information security compliance to improve their protection of PII.

Alternate Theories

General Systems Theory. General systems theory (GST) indicates that certain general principles apply to all systems regardless of their properties (Von Bertalanffy, 1972). Systems are naturally hierarchal. The procedure itself exists on the macro level, while the system's microlevel includes its components. The relationship between system levels is causal, while the system's relationship with the environment is horizontal (Hofkirchner, 2019). According to GST, systems are either open or closed. Available systems elements interact with each other and the environment, while secure systems are isolated from their environments (Vanderstraeten, 2019). Edmonds (2017) wrote that GST is a theory of goal-driven behavior and further suggested that goals are considered the cause of a system's behavior. Individuals adjust their behavior to achieve specific system goals (Edmonds, 2017). GST is appropriate for examining aspects of information security, such as adaptation, communication, control, and self-organization (Dube &

Flowerday, 2018). However, GST is driven by behavior adaptation for goal achievement and was not appropriate for this study.

Dialectical System Theory. Dialectical system theory (DST) addresses the lack of holism, which considers all viewpoints in other systems theories (Zenko et al., 2012). According to Zenko et al. (2012), DST achieves holism through interdisciplinary cooperation. DST supports decision-making in that the manager is presented with information from various sides of the issue, thus giving them a complete picture of the problem (Čančer & Mulej, 2010). DST also takes human behavior into account as part of holistic systems thinking (Ženko et al., 2017). Ženko et al. (2017) used DST to investigate knowledge management and discovered that interdependence and responsibility are necessary for holistic, socially responsible decision making. DST did not apply to this study because it is concerned with cooperation between opposing parties to attain a goal.

Soft Systems Methodology. Checkland (2012) developed soft systems methodology (SSM) for research in various fields, including business, engineering, and social sciences. SSM helps researchers understand complex issues that involve multiple systems and stakeholders (Warren et al., 2019). Torres's (2018) research indicates that SSM's primary focus is investigating complex problems that require action to remedy them. SSM helps in explaining how system stakeholders interact to address problematic situations (Sharma et al., 2019). Fathi et al. (2020) argued that SSM is suitable for investigating complex problems with multifaceted social and human elements. Antunes et al. (2016) used SSM to examine incentive policies and technological innovations in the electricity sector. SSM allowed the authors to create a multicriteria decision support model to help decision makers develop policies that encourage technical innovation in the electricity sector (Antunes et al., 2016). Sutoyo and Sensuse (2018) researched gamification of information systems using SSM. The researchers used SSM to visualize the problem and identify which tools were needed to implement gamification. SSM helps in remembering specific actions required to solve a problem; thus, SSM did not apply to this study.

Contrasting Theories. Grey systems theory is an opposing theory of TAM. Julong developed grey systems theory in 1982 to solve economic, engineering, and social science problems (Nowak et al., 2020). Grey systems theory helps investigate issues with limited available information that is difficult to measure and is subjective (Nowak et al., 2020). Javed and Liu (2017) also argued that the grey systems theory is appropriate for researching topics with small data samples and a degree of uncertainty. Jalali and Heidari (2020) agreed that the grey systems theory helps make predictions with small pieces and limited information. At the same time, Rao and Liu (2017) suggested that grey systems theory involves creating and extracting data from partially known and unknown data to support decision-making and solve problems. Grey system theory deals with problem-solving with little to no information; therefore, grey systems theory does not apply to this study.

Related Studies. Self-efficacy refers to one's belief in accomplishing a goal and is a central TAM factor. An extension of self-efficacy is collective efficacy, which refers to the collaboration and coordination between group members to achieve the collective's goals (Chul et al., 2020). *Information security* is a group effort that requires every member's cooperation within an organization to be effective. Chul et al. (2020) applied the collective agency concept to their information security effectiveness study. The authors found that a workgroup's sense of collective efficacy directly influenced the group's ability to detect, respond, and recover from information security threats. Alshaikh et al. (2018) used TAM to explore the influence of information security monitoring on employees' security assurance behavior. The authors found that employees are more likely to engage in appropriate security behavior when monitored. Alshaikh et al. suggested that information security policies and organizational standards create a company's culture that influences employees' opinions and affects their information security behaviors. Herath et al. (2018) used TAM to understand the relationship between employees' noncompliance with information security policies and environmental factors. The authors discovered that the frequency of security education, training, awareness training, policy awareness, and knowledge of policy violation consequences positively influence employees' information security behavior. According to Herath et al., when employees are aware of security policies and the penalties for violating them, they are more likely to comply with them.

Using TAM as a theoretical lens, Adhikar and Panda (2018) analyzed the relationships between users' privacy concerns and their likelihood of engaging in privacy protection behaviors when using social networks. The researchers evaluated whether users' perceived risk and perceived vulnerability of personal data influence their social networks' security behaviors. The researchers found that users who are confident in their ability to identify and respond to security threats were likely to engage in security conscience behaviors. This finding supports Nguyen and Kim's (2017) assertion that when users have the knowledge and skills to protect information and information systems, they are likely to engage in appropriate security behavior. Additionally, users who were not confident in their ability to identify and respond to security threats were less concerned about data security in social networks. Adhikar and Panda also observed that the perceived consequences of data loss, theft, or compromise influenced users' security behavior in social networks, which aligns with the outcome expectation component of TAM. This observation aligns with Lin and Chang's (2018) findings that outcome expectation influenced users' willingness to share health information in social networks. Adhikar and Panda's study underscored the need for social network companies to inform users of their services' information security implications. When users are aware of information security threats and how to mitigate them, they are likely to engage in appropriate security behavior.

Cuganesan et al. (2018) conducted a quantitative study to investigate the influence of senior management and workplace norms on employees' information security attitudes and self-efficacy. Overall, 338 employees of a law enforcement agency participated in the study. The researchers found that managerial support of information security significantly influenced workers' attitudes towards information security. This finding aligns with Saroia and Gao's (2019) finding that administrative support has a strong relationship with PEOU, which influences usage intention. Yoo et al. (2020) researched information security in workgroups to examine how workgroup information security effectiveness

(WISE) is achieved through workgroup collective efficacy and security knowledge coordination using TAM as a theoretical lens. Yoo et al. also surveyed a law enforcement agency's employee to assess the relationships between collective workgroup efficacy, security knowledge coordination, individual self-efficacy, and workgroup information security effectiveness. Yoo et al. examined whether information security at the workgroup level relates to information security personally. The strength of security at the lowest levels forms the basis for security at higher levels. Yoo et al. found that individual self-efficacy, an external factor of TAM, is a vital WISE element. Yoo et al. discovered that the effect of self-efficacy mediated through the group mechanisms of workgroup collective efficacy and security knowledge coordination; individuals equipped with their security efficacy require coordination for the workgroup to achieve its information security goals. Cuganesan et al. also found that workplace norms directly influenced employees' feelings about information security and that the compliant security behavior of others positively influenced employees' information security self-efficacy.

Similarly, Ramadania and Braridwan found that users' PU, PEOU, attitude, self-efficacy, attitude, and subjective norms are in direct proportion to the level of intent to use online shopping. Cuganesan et al.'s research revealed that the human element of information security is an essential consideration in protecting data. Policies alone are not enough to motivate employees to engage in compliant behavior. Positive role models and security-compliant colleagues significantly influence employees' views and self-efficacy about information security.

Enhancing the human element of cybersecurity is necessary for preventing cyberattacks. Encouraging employees to adopt appropriate security behavior and improving their confidence in doing so supports the external variable of self-efficacy in the TAM. While it is impossible to prevent all cyberthreats, small businesses can make themselves less susceptible by following cybersecurity best practices and guidelines, including enhancing employees' confidence in adopting and implementing appropriate security behavior.

Application to the Applied Information Technology Problem

The study's applied IT problem is that some small businesses lack strategies to protect their customers’ PII against phishing attacks.

Security Policies

Information security policies are one element of an information security strategy that ideally encompasses human factors, technical processes and policies, and data governance (Choi et al., 2018). Paulsen and Toth (2016) described information security policies as the directives, rules, and practices that regulate how an organization handles, distributes, and protects data. Information security policy implementation is challenging for many small businesses. At the same time, Paulsen and Toth concluded that information security policies are needed to protect the information, educate employees, and provide supporting documentation for incident investigations. Sosin (2018) wrote that a robust implementation foundation is necessary to support information security policies. According to Sosin, secure data controls, compliance, security budget considerations, risk management, and security evaluations formulae the basis for adequate information security policies.

Several researchers have reported that some employees lack an understanding of the importance of information security and often fail to comply with information security practices and policies (Alzamil, 2018). Information security guidelines can be confusing for nonIT personnel, leaving them unsure about their responsibilities for protecting data (Sadok & Bednar, 2016).

Sadok and Bednar (2016) found that many organizations did not have clearly defined security policies. Ensuring employees understand and comply with information security procedures requires written policies, well-defined roles and responsibilities, and consistent enforcement. According to Al-Jumaili (2018), small businesses are often vulnerable to information security attacks, risks, and threats due to inadequate security policy practices. Pagura (2019) wrote that many small businesses are susceptible to cybersecurity attacks due to a lack of knowledge, resources, and time to devote to security efforts. Almubayedh et al. (2018) explored information security policies and awareness in small businesses and found that employees were often unaware of their organization's information security policies and best practices.

Failure to enforce information security policies also presents a threat to data. Recent evidence suggested that many organizations have information security policies in place; however, they do not actively enforce them, like not having a policy (Zayed, 2016). Small businesses should ensure all information security policies are disseminated to employees during the onboarding process and subsequently made readily available.

There should also be a system to reinforce the company's stance on information security best practices to remain vigilant in protecting data. Almeida et al. (2018) argued that information security policies are needed to protect the information, which is increasingly becoming one of the most valuable business assets. According to the researchers, the importance of some aspects of the information security policy varied among different business sectors. For instance, financial services organizations were more concerned with internal processes than the IT sector, wherein web services management was of higher importance. Financial services organizations are subject to numerous industry and governmental regulations and laws, which may explain why internal processes are more valuable than information security elements, such as executive summaries and contacts (Almeida et al., 2018). Organizations that are heavily regulated may require more security controls than companies that handle limited amounts of PII or financial information. In sum, the findings of Almeida et al. (2018) and Paulsen and Toth (2016) indicated that the business sector, data type, and information value impact the structure of security policies.

Singh and Gupta (2017) conducted a case study of information security management in small organizations and observed that many small businesses do not have formal information security policies. The researchers' results indicated that participating organizations often lacked role-based access control of data. Everyone has access to everything, and that limited financial, and personnel resources made implementing adequate information security control difficult. Panjwani et al. (2016) also found that access control, user privileges, and security policy implementation are challenging for small businesses. Chinyemba and Phiri (2018) and Bolek et al. (2016) found that companies do not fully implement access control policies, and employees do not always comply with them.

Additionally, Lopes and Oliveira (2016) observed that implementing information security policies was complicated for small businesses and reported that participants felt their organization's security policies were too long and confusing. Njenga and Jordaan (2016) observed that many managers felt that their businesses were too small to worry about information security, so they allowed everyone to access everything. The researchers also found that other managers believed that being overly restrictive was easier than implementing appropriate security controls for protecting sensitive data.

Similarly, Alzamil (2018) and Lopes and Oliveira (2016) concluded that users' lack of awareness of information security policies and leadership's failure to disseminate policies could contribute to security policy implementation challenges. Alternatively, Singh and Gupta (2017) concluded that small businesses should adopt specific guidelines, methods, and approaches to improve their security posture. Implementing information security standards and procedures ensures that data protection methods are consistent across the organization. Additionally, Almubayedh et al. (2018) asserted that organizations should develop a process for measuring information security control effectiveness to identify areas requiring improvement. Raising awareness of information security requires wide dissemination of concise and easily understood information security policies.

Dombora (2019) studied information security management systems (ISMS) to understand why the guidelines and policies of some ISMSs are unenforceable. The researcher created ISMSs quality parameters and development approaches to evaluate their enforceability. Dombora interviewed stakeholders 1 year after they implemented the parameters and guidelines regarding their experiences. Dombora's results indicated that ISMS contained inappropriate or cumbersome rules that created unnecessary expenditures and security gaps; ISMS should comply with industry and legal standards, be written with well-defined roles and responsibilities, and balance risks with resources (Dombora, 2019). Additionally, the research results demonstrated that the overall quality of ISMS improved with implementing the ISMS quality parameters and development guidelines in conjunction with ISO/IEC 27001 based frameworks. Dombora's results support Almubayedh et al. (2018) contention that information security controls can be improved by performing effectiveness assessments. Developing and implementing enforceable ISMS helps small businesses reduce costs and maintain compliance with applicable legal and industrial regulations.

Chinyemba and Phiri (2018) and Bolek et al. (2016) also ascertained that some organizations had information security policies in place, but security managers did not articulate procedures to carry them out. Managers also did not enforce information security controls, and the effectiveness of the information security management system was not evaluated and not documented clearly. Zammani and Razali (2016) studied Information Security Management (ISM) to identify and verify ISM key factors: IS policy, IS procedures, and employees. The authors found that IS policies must clearly define IS roles, responsibilities, and objectives (Zammani & Razali, 2016). Zammani and Razali, like Abbas et al. (2015), research demonstrate needed periodic reviews of information security policies to make sure policies are relevant to the current information security environment.

Similarly, Angraini and Okfalisa (2019) conducted a literature review to identify the challenges and explore current trends in information security policy compliance, which is essential to ensure users adhere to security standards for protecting organizational assets. Angraini and Okfalisa examined articles on information security policy compliance, influencing compliance with information security policies, behavioral intentions, and compliance measurements. Findings revealed there was not enough information to identify the factors influencing the individual choice to comply with information security policies. Angraini and Okfalisa recommended further research to determine the factors that influence individual-level information security policy compliance. Angraini and Okfalisa also discovered that employees are often unaware of information security policies' importance until their company experienced a data breach. Additionally, information security policies should be reviewed and updated consistently to ensure they address current threats (Angraini & Okfalisa, 2019). Measurement tools can help organizations improve information security compliance and measure the effectiveness of existing policies.

Awareness and Training Strategies

Scenario-based training with practical exercises allows users to experience real threats with the chance to apply their newly acquired skills to their responses. Presenting users with real phishing e-mails to improve information security and awareness training is the strategy Slonka and Shrift (2016) used to evaluate the level to which phishing attacks impacted an organization's network.

Conversely, Aldawood and Skinner (2019) argued that information security training should be audience-specific because senior executives face different threats than junior-level employees. Pagura (2019) contended that implementing strict access controls, password policies, and employee awareness training mitigates the risk of unauthorized access to systems and phishing campaigns.

An informal approach to training, such as a focus group or workshop setting, allows learners to exchange ideas and learn from one another. Popescul (2018) conducted an information security workshop to increase cybersecurity awareness among nontechnical employees and found that participants learned with and from one another by sharing experiences and asking questions. When workshop attendees return to their organizations, they can share their knowledge with colleagues, thus increasing the PU of cybersecurity awareness.

Everyone learns differently. For example, some learners prefer classroom instruction to interact with their instructor and classmates, while others learn best through hands-on exercises. With that in mind, Tschakert and Ngamsuriyaroj (2019) developed a mixed-method information security training program to increase awareness of phishing e-mails. Training consisted of a combination of instructor-led classroom training, videos, games, and text-based handouts. Although research participants had an IT background, the variety of training approaches successfully reduced phishing susceptibility while also increasing confidence in their ability to detect phishing e-mails.

Another training approach involves presenting a security policy to a user, explaining the policy's purpose, and testing their policy knowledge through a hands-on exercise. During their research on information security training effectiveness, Ayyagari and Figueroa (2017) informed users about a security policy, showed a video explaining the threats and vulnerabilities associated with the policy, then tested their knowledge using a scenario-based approach. Ayyagari and Figueroa learned that when users understand a security policy's purpose, they are more likely to comply. Likewise, Pham et al. (2017) wrote that understanding the severity of a threat and the likelihood of it occurring may positively influence users' compliance behavior.

User Security Education

Small businesses are often the target of cyberattacks; however, it is possible to reduce the risk of cyberattacks through information security awareness training and education. Phillips and Tanner (2019) observed that some small businesses use information security awareness and information security education synonymously, although they hold different meanings. Phillips and Tanner noted that information security awareness training centers on specific types of attacks, while information security education focuses on policies and general concepts such as phishing. The authors also suggested that information security awareness training be a continual process in that it is updated regularly as new threats are constantly being found and identified. However, information security education is not updated often and is sometimes an occasional activity.

Employees are often the first line of defense for small businesses because their knowledge of information security threats is vital to their overall security posture. When employees are unaware of information security threats, they can fall victim to phishing attacks, resulting in data breaches. According to the SBA (2019), employees opening malicious e-mails are among the primary causes of data breaches for small businesses. As further evidence of employees' vulnerability to phishing, Slonka and Shrift (2016) conducted a study to improve information security training that involved sending spear-phishing e-mails to their clients. Slonka and Shrift found that 20.4% percent of the recipients opened the e-mail, while 12.9% of the recipients navigated through several compromise layers and disclosed their credentials. Recent evidence suggested that through information security and awareness training (ISTA), employees can learn to identify and mitigate common information security threats (Phillips & Tanner; Slonka & Shrift, 2016). Phillips and Tanner (2019) suggested that organizations should invest in ISTA programs because employees often pose the most dangerous cybersecurity threat. Slonka and Shrift wrote that small businesses could improve their employees' ability to recognize phishing e-mails through ISTA programs.

Wenham (2016) contended that ISTA programs are an essential element of information security as informed employees engage in behaviors conducive to protecting data. Training delivered through ISTA programs can potentially reduce employees' likelihood of falling victim to phishing attacks and other well-known threats.

Additionally, Alshaikh et al. (2018) stated that training and awareness programs are necessary for making employees aware of information security threats and risks, which is like Zammani and Razali’s (2016) findings. Other researchers noted that training and awareness programs could inform employees about their roles and responsibilities concerning protecting organizational data (Alshaikh et al., 2018; Zammani & Razali, 2016).

Furthermore, Ključnikov et al. (2019) and Flowerday and Tuyikeze (2016) observed that information security awareness and education and senior management support were the most crucial success factors of information security management. Senior management involvement in information security awareness training ensures that adequate resources for maintaining the program are available. Employees are the first line of defense for small businesses; therefore, investing in developing a comprehensive information security awareness and education program is a worthy expense (Chinyemba, & Phiri, 2018; Phillips & Tanner, 2019). Employees’ lack of knowledge about common information security threats, such as spear phishing, is one reason small businesses are attractive targets for cybercriminals (Prislan et al., 2017; Selznick & LaMacchia, 2018). Protecting sensitive information from cybercriminals requires providing employees with the knowledge, skills, and abilities to defend themselves and their organizations from cyber threats.

Thompson (2016) also highlighted the need for proactivity in data security training. By examining literature concerning information security, Thompson, like Ki-Aries and Faily (2017), found that employees are often the weakest link in the security chain. Through negligence or malice, employees can expose proprietary and personal information to loss, damage, or compromise (Ki-Aries & Faily, 2017; Thompson, 2016). Employees should be knowledgeable and receive continuing education about information security best practices. Data breaches can cause catastrophic damages to a business; therefore, companies must stay abreast of threats to data and computing systems (Thompson, 2016). All companies, regardless of size or industry, are susceptible to the actions of cybercriminals. Companies must realize that planning for a cyberattack before one occurs increases the chances of successfully defending against and recovering from a cybersecurity event (Thompson, 2016).

Several researchers have reported on the importance of information security awareness training. Popescul (2018) argued that arming employees with essential information security skills goes a long way towards protecting data. Uninformed employees often engage in risky activities, such as clicking on links in e-mails, transmitting sensitive data without appropriate protection, writing passwords on sticky notes, and placing them under their keyboards. Simultaneously, ineffective information security training programs do not prepare employees to counter threats to data online and offline. Sadok and Bednar (2016) reported that some small businesses provide generic information about security that is not relevant to the average employee. Likewise, Slonka and Shrift (2016) wrote that numerous companies did not teach their employees how to detect and ignore suspicious e-mails. Popescul asserted that a simple, low-cost awareness training program could help an organization reduce the threat of malware attacks and data breaches. Other researchers discovered that some small businesses do not take responsibility for teaching their employees about information security. Njenga and Jordaan (2016) interviewed small business owner-managers to examine information systems security and reported that some managers believed employees are responsible for staying abreast of information security threats. Similarly, Sadok and Bednar discovered that some small businesses chose to implement technological solutions for securing data without considering the human element of information security. Providing employees with the knowledge and skills to protect data through information security training and awareness adds a layer to an organization's data security defenses.

Technical Strategies

Lack of technical expertise is a common vulnerability among small businesses. Researchers who investigated information security in small businesses found that many organizations did not possess adequate data protection security mechanisms. Iyamuremye and Shima (2018) indicated that network security could exceed small business network security personnel's technical abilities. Njenga and Jordaan (2016) observed that many managers did not implement appropriate security controls because they felt that their businesses were too small to worry about information security. Wenham (2016) argued that technical measures such as installing antivirus software, implementing appropriate access controls, performing data backups, and performing consistent software patching could mitigate the threat of cyberattacks. Pagura (2019) asserted that performing automatic system and software updates and data backups can help prevent attacks and decrease recovery time. Paulsen and Toth (2016) also recommended backing up data to recover if lost, stolen, or compromised. Failure to backup data regularly could cause significant delays in the event of a data breach or natural disaster.

Additionally, many small businesses are unable to purchase information security tools due to limited budgets. To overcome the challenge of financial constraints, Williams (2018) suggested using free, open-source software and technology resources, such as adblockers, to protect their information systems. Ad blockers are generally easy to install as browser extensions, and they can protect users from threats such as third-party tracking, malvertising, and social media button blockage (Williams, 2018). A simple, low-cost security solution like ad blockers is beneficial for small businesses with minimal in-house IT personnel. The time and effort required to deploy and maintain these tools are nominal.

Berry and Berry (2018) examined cybersecurity risk management in small businesses, analyzing data from over 370 surveys sent to small business owners about their risk management approaches regarding cybersecurity threats. Participants have presented questions regarding virus protection, firewalls, backups, IT acceptable use policies, passwords, and other types of security approaches. Similarly, Pagura (2019) argued that small businesses should perform risk assessments to identify potential risks to business networks, information systems, and data as a best practice for preventing data breaches. Berry and Berry found that many small business owners implemented some essential technology risk management tools; however, they also found that participants reported not requiring other basic precautions like solid passwords for accessing information resources. Additionally, participants also reported lacking the knowledge, skills, resources, policies, and procedures to secure their information assets effectively. Berry and Berry suggested that both the private and public sectors continue creating and distributing user-friendly, low-cost, and educational tools to help small businesses with limited resources learn to manage cyber risks. Berry and Berry also recommended that small businesses implement strong password policies and backup data because they are simple, effective, and low-cost methods of reducing the threat of data breaches.

Another technical strategy used to protect data is data classification software. With data classification software, small businesses can protect their data from unauthorized disclosure through clearly marked and defined labels, encryption, and access control (Ritzman, & Kahle-Piasecki, 2016). Technical solutions alone are not enough to secure data. According to Grannemann (2018), a robust information security program that addresses risk management, data governance, threat vulnerabilities, policies, and procedures, along with technical solutions, is needed to prevent data breaches. Rostami et al. (2020) agreed that organizations could not depend solely on technological tools to protect their information and information systems. They also showed that administrative controls, such as information security policies and security awareness training, and technical tools are the building blocks of an effective information security program.

Nontechnical Strategies

Paulsen and Toth (2016) provided several simple, nontechnical controls for securing data in *NISTIR 7621, revision 1 Small Business Information Security: The Fundamentals*. Conducting background checks on employees to understand their character and using computer privacy screens to prevent passersby from seeing data are examples of nontechnical controls presented in *NISTIR 7621 revision 1* (Paulsen & Toth, 2016). Grannemann (2018) supported incorporating security controls found in *NISTIR 7621 revision* one and appropriate formal policies and processes for a robust information security posture. Grannemann also advised organizations to evaluate employee information security awareness consistently, ensure IT staff maintain proficiency in their fields, and continually monitor information security controls, policies, and processes for effectiveness.

One such nontechnical issue involves a lack of publicly available information, not private or proprietary, regarding cybersecurity attacks, threats, and best practices that small businesses can access. Gafni and Patel (2019) conducted a study to determine if there is enough publicly available cybersecurity information available to small businesses to assist them with protecting themselves against cyber threats. The researchers searched websites, news media outlets, and academic journals for information about cybersecurity threats to small businesses. They found there is little publicly available cybersecurity information focusing on small businesses. There are several reasons for the lack of material. First, SMEs may not be aware of data leaks and, therefore, the information does not flow to government agencies, industry officials, or the media for public dissemination. Likewise, Iyamuremye and Shima (2018) argued that small business network security personnel often have limited network security skills. Second, SMEs do not always report data breaches due to fear of financial repercussions caused by fines or lost clientele. This finding aligns with Selznick and LaMacchia's (2018) claim that small businesses could face lawsuits or penalties because of data breaches. Third, news outlets may overlook covering small businesses because the breaches' size is not large enough to capture the public's attention (Gafni & Patel, 2019).

Physical Strategies

A key aspect of information security is physical security. Physical security refers to the physical barriers that prevent or limit access to organizational assets such as buildings, offices, hardware, and servers (Diesch & Krcmar, 2020). Barriers include locked doors, fences, and armed guards. Physical security also calls for protecting internal and external environments, travel activities, and people (Diesch & Krcmar, 2020). Watad et al. (2018) suggested implementing physical security measures to protect facilities that contain high-value IT assets.

Sikora et al. (2017) investigated information security in a small business through a system and software audit. In addition to a questionnaire concerning internal controls, the target organization did not have appropriate physical and logical policies, leaving their information vulnerable to unauthorized use. Findings also revealed no disaster recovery plans or emergency procedures in place, leaving staff confused about their roles and responsibilities during a crisis. There were also no data transmission policies in place, resulting in lost or compromised data (Sikora et al., 2017). The company also failed to develop formal policies addressing data security, data storage, and knowledge management, resulting in the loss of confidentiality, integrity, and data availability (Sikora et al., 2017). Sikora et al.'s findings could help small businesses to improve their information and information systems' security. Small businesses should implement formal policies regarding physical practices to protect information and information systems. According to Paulsen and Toth (2016), information security policies help protect the information, educate employees, and provide supporting documentation for incident investigations. Furthermore, Pagura (2019) maintained that small businesses should perform risk assessments to identify potential risks to business networks, information systems, and data.

Limiting access to sensitive areas to only personnel who require access to perform their duties reduces the likelihood of the unauthorized disclosure of data. Another physical security strategy used by some small businesses to prevent the loss, theft, or damage of information is to lock up mobile devices, laptops, and portable storage devices when they are not in use (Paulsen & Toth, 2016). In conjunction with information security policies, physical security, technical and nontechnical strategies, security awareness, and education add a layer of security for information and information systems.

Transition and Summary

TAM (Davis, 1986) serves as the conceptual framework for the study and will help explain information security strategies for addressing vulnerabilities. The literature offered valuable insights into the information security threats that could lead to data breaches. It is vital that small businesses develop and implement strong information security policies, conduct information security and awareness training, and implement technical, nontechnical, and physical controls to protect data and prevent data breaches.

In Section 1, I provided a list of operational definitions to give readers the precise meaning of terms. I also outlined assumptions, limitations, delimitations, and the study's significance to research practice and social change. In Section 2, I detail how I conducted the research. Discussion topics include my role as the researcher, participants, the research method and design, population sampling, ethical guidelines for the study, data collection instruments, techniques, organization, analysis, and reliability and validity.

Section 2: The Project

In this section, I provide information on the role of the researcher, potential participants, the criteria for selection of participants, population sampling, and research methodology. This section also addresses ethical subjects relating to my study and steps that I took to alleviate such factors. Last, I describe the data collection instruments, data collection approach, data organization techniques, and data analysis and explain issues of reliability and validity in the context of this study. I then provide a transition and summary, leading to the final phase of my doctoral research.

Purpose Statement

The purpose of this qualitative multiple case study was to explore the strategies used by small businesses to protect their customers' PII. The sample population consisted of IT managers located in Alexandria, Virginia. This study's potential social impact is that it may provide strategies to help protect customers' PII, thus minimizing potential financial losses and improving customer trust and confidence.

Role of the Researcher

Qualitative researchers serve as the primary data collection instruments in their studies, and their relationship with participants is collaborative (Billups, 2019). Qualitative data collection sources include observation notes, interview transcripts, memos, and journal entries (Jones & Smith, 2017). In my role as a researcher, I was the interviewer for the study. I was not involved in the activities of the participating organizations. However, I made recordings throughout the interview process and engaged in journaling. Interview notes serve as a record of the researcher's thoughts, feelings, and observations before, during, and after an interview (McClelland, 2017). Transcribing notes after an interview helps with the analysis process in that as they may offer additional insights into the discussion through information such as verbal gestures, prolonged silences, and background noises (McClelland, 2017).

I had no relationships with the partner organizations or with the participants. The experience that I have with information security is that I work in the cybersecurity field. I have also attended webinars and conference sessions about strategies used to protect PII.

I took measures to reduce bias while conducting this study. Qualitative researchers attempt to mitigate personal preferences to correctly interpret study participants' views (Fusch et al., 2018). I minimized personal biases by not imposing my beliefs, opinions, and experiences on the interviewees to avoid influencing this study's findings. Researchers cannot eliminate biases; however, they can minimize biases through reflexivity and bracketing (Borowska-Beszta, 2017). Maintaining a journal throughout the research process can also lessen the tendency. Documenting the research process provides transparency and allows other researchers to verify findings or replicate a study (Mackieson et al., 2019).

I used an interview protocol as a framework for conducting interviews for this study (Appendix B). An interview protocol can help align interview questions with research questions and improve the data obtained from interviews (Castillo-Montoya, 2016). I used the same interview protocol for all participants and asked open-ended, nonleading, semistructured questions to ensure consistency throughout the interviews.

Through semistructured interviews, researchers can explore participants' thoughts, emotions, and choices regarding the phenomena under investigation (Jones & Smith, 2017). I afforded participants ample time to respond to interview questions and offered thoughts on protecting the confidentiality, integrity, and data availability in small businesses. Allowing participants to take the time to reflect on their responses can help them provide thick, rich details about their experiences (Rosenthal, 2016). I used follow-up questions as necessary to ensure that participants elaborated on their responses related to the research question. Follow-up questions help the researcher obtain deep, rich information from participants (Castillo-Montoya, 2016).

The Belmont Report (National Institutes of Health, 1979) served as the ethical foundation and standards for my study. I strictly adhered to the ethical principles detailed in the Belmont Report, which included treating all participants with respect and protecting them from any form of harm (National Institutes of Health, 1979). I also provided participants with all information needed to make an informed and voluntary agreement to participate by giving complete and honest disclosure as suggested by the National Institutes of Health (1979). I advised participants of their ability to withdraw from the research at any time. Furthermore, if other parties' permissions were needed to protect participants from risk, there would also be outcomes and procedures within the process of participant selection (National Institutes of Health, 1979).

I completed the Doctoral Student Researchers Basic Course offered by the Collaborative Institutional Training Initiative (CITI). My CITI certificate is in Appendix D.

Participants

Qualitative research is appropriate for answering questions related to the “who,” “what,” and “where” of experiences or events (Kim et al., 2017). Obtaining multiple perspectives about a phenomenon from people with personal experience contributes to deep understanding (Wu et al., 2016). The target population for this study was IT managers working in small businesses. The ideal candidate had worked with a small business that experienced the loss of customers’ PII. Qualitative descriptive researchers can achieve data saturation with three to five participants (Magilvy & Thomas, 2009). After receiving Institutional Review Board (IRB) approval, I contacted candidates via e-mail to inform them about the study and ask them for a convenient time to reach them via phone. The purpose of the phone conversation was to establish rapport with the candidate and address any questions or concerns about the study. I used purposeful sampling for this study. The ideal number of cases for this study was eight cases.

In qualitative case study research, it is possible to achieve data saturation with one case. The research question, data collection technique, data type, and variety of participants determine sample size (Moser & Korstjens, 2017). Convenience sampling is a selection technique in which the researcher chooses participants who are easily accessible (Naderifar et al., 2017). Convenience sampling is appropriate when the researcher cannot follow purposeful sampling protocols (Owen-Smith & Coast, 2017). According to Setia (2017), sampling is purposive when participants are chosen based on their ability to answer the research questions. Employing two or more purposeful sampling techniques can enhance a sample’s quality and diversity (Benoot et al., 2016). I made every effort to develop and maintain all participants' trust by ensuring their comfort, maintaining complete transparency through every phase of the interview, and allocating the appropriate time and effort to build trust. After receiving IRB approval (Walden IRB approval no. 11-01-21-0523033), I selected and invited potential participants to participate in the study. My IRB approval number is I emailed an informed consent form to volunteering participants. The informed consent form detailed the study purpose, participation criteria, my role as the researcher, the withdrawal process, the disclosure of incentives, data safeguards, and the intention to publish findings. I also informed participants that participation in the study was voluntary. Participants had the right to withdraw from the study at any time before data analysis without cause by contacting me via email. I followed the Walden University IRB ethical and legal requirements to ensure that no harm or risks came to the participants associated with my research.

Research Method and Design

I chose the qualitative research methodology, which includes a multiple case study. The qualitative multicase research design provided me with a deep understanding of strategies used to protect customers' PII. I also ensured that the research methodology and design aligned with the research question for my study.

The qualitative multicase method was appropriate for this study because it explored the information security strategies used by small businesses to protect their customers' PII. Data gathered from small businesses through semistructured interviews helped in obtaining a deeper understanding of strategies that small businesses use to protect their customers’ PII.

Method

I used the qualitative multiple case study method for this investigation. After considering the quantitative, qualitative, and mixed-method research approaches, I chose this study's qualitative research methodology. Qualitative research focuses on events, individuals, and contexts (Gerring, 2017). According to Murshed and Zhang (2016), qualitative inquiry helps in gaining a deep understanding of a phenomenon when knowledge is limited. Murshed and Zhang argued that data collection in qualitative research involves direct interaction with study participants and context immersion and is recounted in detailed descriptions. Likewise, Colorafi and Evans (2016) asserted that qualitative research findings enable understanding by presenting results in everyday factual language.

A qualitative research approach was chosen for this research study because my aim was to explore cases to gain deeper insight into the information security strategies used by small business managers to protect PII. Hesse-Biber (2020) wrote that quantitative exploration is objective and relies on numerical/statistical findings as evidence of a single reality. Quantitative methods are suitable for answering questions such as “how many,” “where,” “when,” “who,” and “how” (Apuke, 2017). Because of data classification’s reductive nature, it is impossible to gain a deep understanding of a subject through quantitative research (Savela, 2018). Results from quantitative examinations can reveal behaviors and trends; however, they do not offer insight into the behaviors' motivation (Goertzen, 2017).

Focus groups, interviews, and surveys with open-ended questions can help clarify information not easily explained numerically (Goertzen, 2017). I did not choose the quantitative research approach because this study's purpose was not to understand the relationship between variables or to validate or disprove hypotheses. Furthermore, mixed-method research combines elements of both qualitative and quantitative methods. Researchers create a coherent research design using an existing methodology, merging current processes, or mixing different methodologies (Schoonenboom, 2018). Mixed method researchers must reach data saturation in all methods, which is time and resource intensive. Mixed methods research requires meeting the reporting standards of quantitative and qualitative approaches (Levitt et al., 2018). I did not select a mixed method for this study due to time and resource constraints.

Research Design

The study involved an exploratory multiple case study, which proved suitable for exploring strategies that small businesses in Alexandria, Virginia, use to protect their customers' PII. Researchers use case studies to examine individuals' experiences in their natural setting (Harrison et al., 2017). Harrison et al. (2017) contended that case study findings can lead to a deep understanding of behaviors, practices, processes, and relationships in context. According to Ridder (2017), case study findings are not generalizable, sampling is nonrandom, and environmental conditions are uncontrolled.

Ridder stated that case study data analysis consists of looking for patterns within and among cases.

Further, case study data collection continues until no new patterns or themes emerge. Case study findings are typically narrative in form and consist of detailed descriptions of the case's key elements. (Hancock & Algozzine, 2017). Ethnographical researchers examine culture and its influence on members' behavior (Rutberg & Bouikidis, 2018). Mohajan (2018) described ethnography as the prolonged observation of a cultural group perceived by its members. Phenomenology helps study an event as told by people who lived through the experience (Rutberg & Bouikidis, 2018).

I examined multiple sources of data in my research study to achieve data saturation. I interviewed participants from small businesses until no new patterns or themes emerged. Interviewing people with firsthand knowledge of a phenomenon is essential for obtaining an in-depth understanding of their experiences (Rosenthal, 2016). I maintained a record of all data collected, and after I determined that there was no new information revealed, I assessed the achievement of data saturation.

Population and Sampling

The purpose of this qualitative multicase study was to explore security strategies used by small business IT managers who had protected their customers' PII from phishing attacks. The inclusion criteria were necessary to focus my efforts on a specific population for my research study. My research study population consisted of IT managers working in small businesses in Alexandria, Virginia. IT managers are IT professionals responsible for protecting their customers' PII through the development and implementation of organizational procedures, policies, and preventative techniques (Billingsley, 2019; Haqaf & Koyuncu, 2018).

I chose purposive convenience sampling for my research study. Purposive sampling is a technique in which participants' predefined characteristics align with the purpose of the study (Andrade, 2021). Campbell et al. (2020) wrote that purposive sampling improves research trustworthiness by aligning the sample to the goals and objectives of the study, thereby improving the study's accuracy and reliability of the data and results. Bhardwaj (2019) purported that an advantage of purposive sampling is that participants possess the appropriate knowledge to help researchers achieve their research objectives. According to Etikan et al. (2016), convenience sampling is a sampling technique in which participants must meet specific criteria such as easy accessibility and proximity to the researcher. With convenience sampling, the primary concern is generalizability. Etikan et al. also wrote that participants are selected based on their ability to contribute thick, rich information to the study in purposive sampling. I selected participants within my network who had the skill and experience to protect PII from phishing attacks. The study population was all IT managers in Alexandria, Virginia. The selection of the population aligned with the purpose of the research. The sample size for the study was eight IT managers in my network who had experience and knowledge of the strategies used for protecting customers' PII from phishing attacks. These eight IT managers represented the eight cases in this multiple case study. I iteratively conducted interviews and examined publicly available information security policies, training presentations, and training techniques for data triangulation, ceasing these efforts when no new information or themes appeared. I evaluated the information collected from interviews and publicly available information security training presentations and training techniques to check for data saturation from each participant. I then compared that information among participants. I conducted member checking using follow-up interviews with the participants to verify my understanding of their statements in the initial interviews. Data saturation is achieved when no new themes are established.

Ethical Research

Upon IRB approval, I selected and invited potential participants to participate in the study. I emailed an informed consent form to volunteering participants. The informed consent form detailed the study purpose, participation criteria, my role as the researcher, the withdrawal process, the disclosure of incentives, data safeguards, and the intention to publish findings. I also informed participants that participation in the study was voluntary. Participants had the right to withdraw from the study at any time before data analysis without cause by contacting me via email. I followed the Walden University IRB ethical and legal requirements to ensure that no harm or risks came to the participants associated with my research. Research participants did not receive any incentives, payments, or rewards for participating in the study. Participants remained anonymous. I assigned each participant a pseudonym such as P1, P2, or P3. I did not use any personally identifiable information or organization names throughout this study. The data have been stored securely per the IRB requirements outlined by Walden University.

I will maintain exclusive access to all data on a password-protected, encrypted external drive and lock in a fireproof safe for 5 years to protect participants' confidentiality. Five years from the date of publication of this study, all collected research data on the external hard drive will be permanently destroyed, including any audio recordings and paper records as detailed in the Ethical Research section, in keeping with Walden University IRB requirements regarding informed consent.

Data Collection

Instruments

Rutberg and Bouikidis (2018) stated that the researcher is the data collection instrument in qualitative research. I was the primary data collection instrument for this study. I used semistructured interviews for data collection. I used six open-ended questions within the data collection instrument. According to Rutberg and Bouikidis, in-depth interviews can lead to thick, rich data collection as the researcher can identify additional areas to explore through follow-up questioning. To ensure credibility and reliability, I asked each participant the same interview questions. I applied member checking during the interview process to achieve research reliability, validity and reduce bias. Member checking is a credibility technique in which participants are given data or findings and asked to verify the correctness and truthfulness (Birt et al., 2016). I used transcription checking to verify the accuracy of participants' responses to interview questions. I provided participants an e-mail summary of my interpretation of their interview responses to accurately capture the participants' responses. I used an interview protocol to maintain consistency throughout this qualitative research study. The interview protocol consists of ensuring interview questions align with the research questions, developing open-ended questions to elicit explicit details, and member checking

(Castillo-Montoya, 2016). Pre-interview activities consisted of a personal introduction, verification of proper completion of informed consent forms, disclosure of interview recording, and study confidentiality review. Through semistructured interviews, participant observation with notetaking, the reliability, validity, and overall quality of the research study improves.

Data Collection Technique

Data collection commenced following IRB approval. Participants who met the research criteria received an e-mail invitation to participate in the study. Once a participant agreed to participate in the research, the participant received a consent form to participate in the study. The consent form detailed the withdrawal process, the disclosure of incentives, and data safeguard. Once I received consent via e-mail, I requested a convenient date and time for a telephone interview. All participants received a copy of the interview questions via e-mail before the interview.

Interviews were the primary data collection technique. Data comes from various sources such as focus groups, interviews, field observations, documents, audio, video recordings, and other multimedia sources in qualitative research (FitzPatrick, 2019). I used open-ended questions to capture the necessary data to address the research question. According to Bengtsson (2016), in-depth face-to-face interviews allow the researcher to deepen the discussion through follow-up questions, generating thick, rich data. I preserved participants' privacy by conducting interviews in an empty room with the door closed to prevent our conversation from being overheard by others. I took notes before and after each interview. Interviewer notes offer additional insight into interviews, such as participant's gestures and emotions and my own experiences during the process (McClelland, 2017). I recorded all interviews using a digital recorder. After the interviews, I transcribed the recordings using NVivo transcription software. Transcribing the interview allowed me to develop a deep understanding of what the interviewee was saying, which assisted with data analysis (FitzPatrick, 2019; Saldaña, 2015). I reviewed the transcribed text while listening to the audio recording to ensure accuracy and summarized my interpretation of member checking responses.

Triangulation helped to enhance the accuracy of interpretation. Triangulation consists of collecting and analyzing data from various sources using multiple methods to identify a convergence of results (FitzPatrick, 2019). I used methodological triangulation to compare the information presented in the interviews with data found in open-source documents that could detail security policies and training methods used to protect PII from phishing attacks. Open-source documents includes information security policies, guidelines, and training plans. Triangulation contributes to the accuracy of a research project as it involves using numerous theories, data sources, or research methods to obtain a complete picture of a phenomenon (Moon, 2019).

Each participant received an individual summary of my transcript's interpretation for review to ensure accurate representation and credibility (FitzPatrick, 2019). I asked participants to edit, clarify, elaborate, and comment on the narrative summary to ensure I understood their viewpoint. In the data analysis, I incorporated feedback from each participant and confirmed themes that emerged in the study. Purposeful sampling is an appropriate technique for qualitative descriptive research (Lambert, & Lambert, 2012). A qualitative descriptive research design is a suitable method for determining the who, what, and why of a phenomenon (Kim et al., 2017). Researchers may understand a phenomenon through rich descriptions offered by study participants (Magilvy & Thomas, 2009). The main objective of qualitative research is to gain a deep understanding of a phenomenon through the experiences of those who lived through the phenomenon (Castleberry, & Nolen, 2018). Thematic analysis helps analyze data collected through qualitative research (Castleberry & Nolen, 2018). Lemon (2017) suggested applying mindfulness to qualitative research data collection as a means of remaining present and objective throughout the process. Qualitative researchers can mitigate biases by selecting an appropriate data collection method (Fusch et al., 2018). Fusch et al. (2018) offered four types of triangulations, (a) data triangulation, (b) investigator triangulation, (c) theory triangulation, and (d) methodological triangulation. Rosenthal (2016) argued that to understand a phenomenon, the researcher needs to talk to people who have had the experience the researcher wants to learn.

Data Organization Techniques

I used two audio recorders to record all interviews of the participants as a precautionary measure. Two audio recorders were necessary to preserve data should one of the recording devices become damaged, lost, or malfunctioned. I used data organization techniques to construct, codify, organize, and securely store data collected during this study. I used NVivo 12 qualitative analysis software to manage and organize this study's information. NVivo allowed me to analyze, visualize, and organize data to uncover any patterns it contains. NVivo software can manage resource materials in various formats or file types. The file types used in this study included spreadsheets, documents, portable document format (PDF), and web pages. Using NVivo I transcribed, and stored audio files created from the participant's interviews. I used Microsoft Word to create consent forms and document the interview process with participants. After each recorded interview, I used NVivo 12 to transcribe the interviews and saved each transcript in a case. Cases in NVivo 12 are containers that store pertinent data needed for analysis. I labeled the cases using the format Case 1, Case 2, Case 3. I managed each transcript in a Microsoft Word document and removed participant's personally identifiable information. I stored the member-checked transcripts, research log, and archival documents in a folder labeled for each case study.

Next, I organized all collected and reviewed data into categories using NVivo. NVivo can assist the researcher in coding, auditing, and organizing data (O'Kane et al., 2021). NVivo software can organize information according to case and theme. NVivo allows for manually creating codes while examining data content. I took interview notes in a research log to contribute to my study's confirmability, reliability, and validity. I used a reflective journal to document my thoughts, feelings, reactions, and reflections on what I experienced during the study. In qualitative research, reflective journals are tools that promote self-awareness and evaluation (Sahin et al., 2019). Reflective journals can also help researchers identify weaknesses and create strategies for improvements (Sahin et al., 2019). I used reflective journals to document the events and thoughts experienced during the study. I stored the interview recordings, transcripts, and all notes on an encrypted hard drive only accessible by me. I will destroy all data collected during this study after 5 years from the completion date.

Data Analysis Technique

In this section of the research study, I outline the data analysis techniques I used to analyze data collected about information security strategies to protect the confidentiality, integrity, and availability of data and prevent data breaches. The data analysis stage involves thematic exploration of data collected through observations, interviews, and other qualitative data collection techniques (Yin, 2013). After the transcribed interview was reviewed and accepted by each participant as accurate, I performed thematic analysis on all other data collected during this study using NVivo version 12. I used data triangulation to verify findings and improve the quality of the research.

Coding

When conducting data analysis, I was the instrument and judged coding, theming, decontextualizing, and re-contextualizing the data. As a result, I needed to be objective during analysis and allow the data to speak for itself. I used the audio recordings and visual transcripts from participants' responses in the interviews to discover common themes about the topic under study to analyze the data. I then reviewed all themes and ensured all names were defined. Finally, I created a report on the themes and codes.

The transcripts from the interviews were coded or deconstructed into manageable code categories for analysis. Coding helps the researcher make sense of their data concerning the research questions (Elliott, 2018). Coding is a way of labeling, mapping, or tagging data that are relevant to a particular point (Elliott, 2018). Coding may be performed manually or with qualitative data analysis software such as NVivo. NVivo can assist the researcher in coding, auditing, and organizing data (O'Kane et al., 2021). NVivo software can organize information according to case and theme. NVivo allows for manually creating codes while examining data content. I used different coding labels to organize the themes while conducting data analysis.

When the transcripts were coded into categories, the codes were placed into categories to create a clearer picture of the data. I used the inductive coding method; the codes emerged based on the present data. After I gathered all the data from the interviews, I began coding the common responses that emerged from the data. To ensure the accuracy of the coding process, I extracted the most accurate and relevant codes from the data.

Reliability and Validity

Reliability

The following section of the study introduces reliability and validity for qualitative research. Lincoln and Guba (1985) proposed four criteria for evaluating the reliability of qualitative research (a) credibility, (b) transferability, (c) dependability, and (d) confirmability.

Validity

According to Cypress (2017), validity refers to the investigative rigor used in qualitative research. I used semistructured interviews for data triangulation. Collecting rich data from participants is vital for obtaining a complete understanding of an event or experience (FitzPatrick, 2019). Selecting an appropriate methodology and sample population to explore a phenomenon is required for ensuring validity (Mohajan, 2017). Validity occurs by guaranteeing the achievement of dependability, confirmability, transferability, and credibility.

Dependability

In qualitative research, dependability refers to achieving consistent results when using a specific research method. Member checking helps establish trustworthiness. Member checking allows participants to provide feedback on any data collected and offer additional information if necessary (Ellis, 2019).

To ensure that a study is repeatable, researchers can create an audit trail of the data collection process and study methods (Forero et al., 2018). I documented the entire data collection process. Participants should have an opportunity to review their interview transcripts along with the researcher's interpretations to validate findings (FitzPatrick, 2019). Data triangulation and member checking assure the accuracy, dependability, and credibility of research (Jordan, 2018). I used data triangulation and member checking to ensure this study's accuracy, trustworthiness, and credibility. Data triangulation is the process of collecting data through multiple sources to obtain a complete assessment of a phenomenon (Moon, 2019). I used an interview protocol to promote dependability further.

Credibility

Credibility in qualitative research refers to the findings' truthfulness and accuracy (Hammarberg et al., 2016). I established credibility through the ethical treatment of research participants and integrity in data collection, analysis, and presentation of findings (Abdalla et al., 2018). To ensure this study's credibility, I adhered to the research method, design, data collection, and analysis. I asked participants the same interview questions. According to Lincoln and Guba (1985), member checking is an essential technique for establishing credibility as participants can confirm the accuracy of the researcher's interpretation of their experiences. I employed member checking by reviewing my interpretation of individual interview responses with each interviewee for accuracy. Two methods for creating credibility are extended engagements with study participants and reflective journaling (Connelly, 2016). Triangulation is the process of examining a phenomenon through multiple viewpoints to achieve a deeper understanding of the research topic and minimize biases (Abdalla et al., 2018). I ensured the credibility of this study through triangulation. Triangulation uses multiple data sources, research methods, or theories to ensure the accuracy or comprehensiveness of a research study (Moon, 2019).

Transferability

Transferability in qualitative research refers to the ability to transfer data results to other settings. Selecting qualified participants to answer the research questions is one approach for generating valid and generalizable results (Weis, & Willems, 2017). Daniel (2019) wrote that thoroughly explaining delimitations helps with achieving transferability. Daniel also suggested including the researcher's rationale for selecting data collection and analysis methods, along with any challenges they faced during research. Similarly, Maxwell (2020) reasoned that transferability is possible when the researcher provides enough details about the contexts, meanings, settings, population, and study processes. The reader can determine the likelihood that results apply to a different location or people.

Confirmability

To achieve confirmability, I documented the entire data collection process, including all notes taken and recordings. I used triangulation to promote confirmability. I also recorded and reviewed transcripts and conducted member checking and note-taking during the interview process.

Data Saturation

I examined multiple data sources in my research study to achieve data saturation. Because this is a multiple case study, I interviewed participants from various organizations until I no longer discovered new information, patterns, or themes. I maintained a record and awareness of all collected data. I reached data saturation when results became redundant. I achieved data saturation using a purposive sample size for the study. The utilization of purposive sampling supported data saturation by identifying participants with rich and detailed experiences in data security within each case study.

Transition and Summary

In Section 2, I presented the research method and design that I used to conduct this study. I also outlined my role as the researcher, study participants, population, sampling, ethical guidelines for the research, data collection, reliability, and validity. I also described data collection instruments, data collection techniques, and data analysis techniques. Additionally, concerning reliability, and validity, I detailed dependability, credibility, transferability, confirmability, and data saturation.

In Section 3, I elaborate on the qualitative study focusing on the overview of the research, presentation of the findings, application to the applied information technology problem, and implications for social change. I then present recommendations for action and further study. Last, I offer personal reflections for this qualitative study.

Section 3: Application to Professional Practice and Implications for Change

Introduction

The purpose of this qualitative multiple case study was to explore the strategies that IT managers use to protect PII from phishing attacks. I collected data for this research by conducting semistructured interviews with eight IT managers and reviewing open-source information security documents. Four themes emerged from the data analysis: (a) users are the first line of defense in protecting PII, (b) preventing phishing attacks is challenging for small businesses, (c) users are a challenge in protecting PII from phishing attacks, and (d) user awareness and training is the best defense against phishing attacks. In this section, I discuss the findings, applicability to professional practice, implications for social change, recommendations for action, and recommendations for future research, ending with a conclusion.

Overview of Study

I commenced this study to understand how some IT managers in small businesses protect PII from phishing attacks. Small businesses are attractive targets for cybercriminals due to their lack of robust security (Wolf et al., 2021). The data I collected indicated that users are the greatest asset and primary threat to information security. Alzamil (2018) noted that some employees lack an understanding of the importance of information security and often fail to comply with information security practices and policies. Chinyemba and Phiri (2018) made a similar observation and stated that employees do not always comply with access control policies. One of the biggest challenges is making employees aware of information security threats while also ensuring that they consistently engage in appropriate security behavior. Phishing techniques are constantly evolving, and to stay abreast of these threats, security managers must be vigilant. Small businesses can reduce their risk of suffering data breaches via phishing attacks by offering information security training and developing, implementing, and enforcing strong security policies and processes.

Presentation of the Findings

I conducted semistructured interviews with eight participants, performed member checking to validate the data, and used purposeful sampling to select participants. Purposeful sampling supports a researcher's ability to select desired qualities in participants (Andrade, 2021). I utilized TAM and UTAUT as the conceptual and supporting frameworks for this study. My goal was to determine if strategies for protecting PII and preventing data breaches through phishing attacks aligned with the PEOU and PU concepts outlined within TAM and UTAUT. Within the context of these frameworks, PU refers to IT managers' belief that information security policies, processes, and technology will enhance their ability to protect data from various threats. PEOU refers to the simplicity of using security technology and complying with information security processes and policies.

I found evidence that the cases in this study employed elements of both TAM and UTAUT as part of their data protection strategy. In addition to conducting semistructured interviews, I collected publicly available documents related to information security policies. I performed triangulation by comparing data collected through the semistructured interviews and publicly available information security policies. I transcribed the interview recordings to Word documents, sanitizing files to remove filler words, time markers, and irrelevant interview discussions. I also added written responses to follow-up questions to the appropriate participants' Word document. I uploaded the collected documents and sanitized files into NVivo 12 for analysis. Data analysis yielded four dominant themes: (a) users are the first line of defense in protecting PII; (b) preventing phishing attacks is challenging for small businesses; (c) users are a challenge in protecting PII from phishing attacks, and (d) user awareness and training is the best defense against phishing attacks.

All participants were IT managers with experience in information security in small businesses. IT managers are responsible for storing, processing, transmitting, and protecting sensitive information. Sensitive information refers to organizational, employee, customer, partner, and vendor information. Therefore, developing and implementing effective information security strategies is essential for IT managers.

In the following section, the four themes that emerged during the data analysis phase are evaluated against the review of the literature and examined through the lens of Davis's (1989) TAM and Venkatesh et al.'s (2003) UTAUT, which served as the conceptual and supporting frameworks for this study.

Theme 1: Users Are the First Line of Defense in Protecting Personally Identifiable Information

The theme of users being the first line of defense in protecting PII was the primary theme to emerge during the data analysis stage of this study. The findings of this study demonstrate alignment with existing literature in the concept of users being a crucial element of information security.

All participants indicated that users were assets and liabilities when protecting PII from phishing attacks. Users may be a threat to information security through inexperience, negligence, or malicious intent. This finding aligns with that of Thompson (2016) and Ki-Aries and Faily (2017) that users are the weakest link in the information security chain. Employees can expose proprietary and personal information to loss, damage, or compromise (Ki-Aries & Faily, 2017; Thompson, 2016). Informed users who consistently engage in appropriate security behaviors can reduce the risks of data loss through phishing attacks.

When examining this theme through the lenses of TAM and UTAUT, creating and implementing simple policies, processes, and procedures can increase users' compliance and reduce the likelihood of them engaging in inappropriate security behaviors. PEOU is a pillar of both TAM and UTAUT. PEOU is the simplicity associated with adopting a technology. To et al. (2021) suggested that pleasant and straightforward experiences increase users' likelihood of adopting new technology. Likewise, the UTAUT behavioral factor EE aligns with this theme. According to Puriwat and Tripopsakul (2021), EE refers to the ease of using a system. EE relates to the effort needed to develop, implement, and maintain PII policies, processes, and technologies.

Table 1

Frequency of First Major Theme in Participant Responses and Documentation

	Participant		Document	
Major theme	Count	References	Count	References
Users are the first line of defense in protecting PII	8	42	11	150

Theme 2: Preventing Phishing Attacks Is Challenging for Small Businesses

The theme of preventing phishing attacks being challenging for small businesses was the second theme to emerge during the data analysis stage of this study. The second theme that emerged from interviews and collected documents from this study aligned with the findings in the literature. Phishing attacks can occur through email, text messages, or phone calls. Defending against phishing attacks is difficult for small businesses for various reasons. Five participants reported that they were vulnerable to multiple kinds of phishing attacks. The most frequently noted attack was email phishing. P6 described email phishing attacks as "harmless-looking emails that contain links." P8 noted spoofing attacks, wherein customers are asked to enter credentials into a webpage that looks legitimate, but it is not. Four participants indicated being vulnerable to spear-phishing attacks. P7 and P2 pointed out that smishing is a common phishing tactic. P7 described smishing as "phishing attacks that come in the form of text messages." Table 2 presents the most common types of phishing attacks.

Table 2

Most Common Phishing Attacks

Phishing attacks	Number of participants
Email phishing	6
Spear phishing	4
Smishing	2
Whaling	2
Phone calls	1
HTTPS phishing	1

Note. Participants reported multiple types of attacks.

Table 3

Frequency of Second Major Theme in Participant Responses and Documentation

	Participant		Document	
Major theme	Count	References	Count	References
Preventing phishing attacks is challenging for small businesses	8	12	2	64

Five participants listed more than one challenge to phishing attack prevention, including the rapidly changing nature of kinds of phishing attacks. For three participants, the costs associated with phishing prevention were a challenge. “Top email filters can cost money to monitor,” said P2. Similarly, P7 said, “Another challenge that I had to deal with was the lack of funding to implement these strategies. I have often seen [organizations] take the cheaper option as it pertains to providing funding to help protect customers’ PII.” P8 said, “the challenges of lack of financial resources” were a problem.

Another challenge to phishing prevention was technology. P3 listed several technological challenges, including email and web filters, which do not always reduce phishing attacks, “attack vectors are polymorphic,” and workstations become susceptible to phishing attacks when patches are not up to date. According to P8, the challenge was “personnel resources and personnel skills relative to the strategies of building a security plan.”

The theme of preventing phishing attacks being challenging for small businesses aligns with existing literature regarding challenges associated with preventing phishing attacks. Legg and Blackman (2019) contended that defending against spear phishing campaigns is challenging because they are not easily detected by users or technical protections such as spam filters. Bhardwaj et al. (2020) agreed that traditional email security tools such as spam filters are ineffective in preventing spear phishing attacks. Bhardwaj et al. also argued that novice and experienced users could fail to recognize spear phishing attacks due to their rapidly evolving tactics. Defending against phishing attacks requires a robust user awareness and training program to help users recognize spear phishing emails. Spam filters are not well suited in identifying the minute details that distinguish legitimate emails from deceptive spear phishing emails.

Within the context of TAM and UTAUT, the concept of preventing phishing attacks being challenging for small businesses aligns with the TAM factor PU and the UTAUT element PE. PU refers to the effectiveness of user awareness and training along with technical security tools to prevent phishing attacks. PE refers to the belief that user awareness and training with technical security tools will prevent data loss through phishing attacks. Usage of technical tools and user training to prevent phishing attacks aligns with Sengkhyavong (2019) in that PU is a significant factor in IT managers' decision to support a specific technology. Small businesses' employment of user awareness and training and spam filters supports Puriwat and Tripopsakul's (2021) assertion that PE refers to the extent to which users believe that a system will help them perform their jobs.

Theme 2 focused on the types of phishing attacks small businesses face and the challenges to protecting customers' PII. However, the most prominent challenge that participants noted was users. I created the following theme, Theme 3, to focus solely on users as a challenge to protecting customers' PII.

Theme 3: Users Are a Challenge to Preventing Phishing Attacks

According to six participants, users' lack of knowledge and understanding of policies presented the most significant weakness in protecting against phishing attacks. P1 described the challenge of "teaching users to identify suspected phishing emails." Similarly, P3 reported the challenge of training people to "effectively recognize phishing campaigns.” P6 added to the challenges that users present, stating, “Users do not always abide by security policies,” but also noted that when users know that security tools are in place, they “become complacent about security.” P7 explained,

> Some of the challenges that I have experienced often originate with the users. A lot of my users do not like some of the policies that I have to enforce in order to protect them. I often hear that our policy on password complexity and minimum character length is too strict.

In addition to the threats to customer PII and challenges to securing PII addressed in Theme 3, users presented the biggest challenge to securing customers’ PII. In addition, participants reported that users were the primary consideration when designing systems to protect PII. P1 reported two primary considerations, user awareness and user education. P2 said, “You have to think about the customers involved when developing strategies.” In addition, Participant 6 noted that “security technology should not interfere with users’ ability to access information and perform their jobs.”

Access to data was also a primary consideration. Participant 5 said that it was important to limit “physical access to data.” Participant 6 explained, “Access is a consideration when implementing strategies to protect PII.”

The theme of users being a challenge to preventing phishing attacks supports existing literature on users’ lack of awareness of phishing attacks. This theme also aligns with existing literature on users’ failure to comply with information security policies. Ramsey and Seyyedhasani (2021) asserted that users’ awareness of cyberthreats, strong password policies, and physical and logical data access controls are essential steps towards reducing the risk of data breaches. Similarly, Panjwani et al. (2016) found that access control, user privileges, and security policy implementation challenge small businesses. Das et al. (2019) wrote that users may unwittingly cause a data breach by failing to comply with security procedures. Small businesses may reduce the threat of data breaches through both technical and nontechnical measures. Increasing awareness of cyberthreats and implementing data access controls, strong password policies, and information security policy enforcement are vital to protecting data from internal and external threats.

When viewed within the context of TAM, the theme of users being a challenge to preventing phishing attacks aligns with the TAM factor PEOU and the UTAUT element PE. PEOU refers to users' perception of the simplicity associated with complying with information security policies and using security technologies. Cuganesan et al. (2018) argued that protecting data requires considering the human element of information security. Razmak and Bélanger (2018) asserted that users are more likely to use an information system if they develop a positive relationship with it. PE refers to implementing information security technology that does not interfere with users' ability to access information and perform their duties. If a system is cumbersome or impedes users' ability to perform their jobs, they will likely reject it (Peterson et al., 2020). Small businesses can improve their security posture by implementing technology and policies that are easy to use, perform as expected, and do not inhibit access to information.

Table 4

Frequency of Third Major Theme in Participant Responses and Documentation

	Participant		Document	
Major theme	Count	References	Count	References
Users are a challenge in protecting PII from phishing attacks	6	23	7	129

Theme 4: Training Users Is the Best Line of Defense Against Phishing Attacks

Themes 2 and 3 presented data showing the challenges to securing small business customers' PII, and that, according to participants, users were the biggest challenge. Users were also participants' primary consideration when creating security systems to protect PII. However, as users represented a security threat, users could be an asset to preventing phishing attacks with appropriate training. According to Adil et al. (2020), user training in conjunction with technical methods is a practical tool for preventing phishing attacks. Likewise, Sadiq et al. (2021) argued that users could avoid falling victim to phishing attacks by staying abreast of phishing tactics and techniques. Prevention efforts are focused on providing regular and thorough training to users, including simulations of the impact of attacks. User awareness training taught users to identify phishing attacks of various forms and use intuition and best practices to guard against attacks.

P6 said, "User training is the best defense," indicating the importance of educating users to recognize phishing emails, which were the most identified type of attack in theme 2. P3 explained,

> Phishing awareness training has become the routine within the organization. All employees are required to take the training on an annual basis. In addition, there are phishing campaign exercises every quarter. Individuals who fall victim to those exercises are usually provided extra remedial training.

Several participants stressed the importance of training users as the first line of defense against phishing attacks. P7 said, "The first thing I do is educate the customers on what a phishing attack is. I believe it is imperative that they know the dangers of these attacks." However, participants did report implementing other forms of data protection. Most participants used a combination of technical and nontechnical protection methods to guard against phishing attacks. I present the types of data protection methods in Table 5.

Table 5

Types of Customer Protection

Protection	Number of participants
Training and educating users	5
Controlling access	4
Filters	4
Secure storage	2
Strong password	2
Encryption	1
Multifactor authentication	1
Software	1

Table 6

Frequency of Fourth Major Theme in Participant Responses and Documentation

	Participant		Document	
Major theme	Count	References	Count	References
User awareness and training is the best defense against phishing attacks	8	54	9	28

Six participants described regular, ongoing training of customers to prevent phishing attacks. P2 said they implement "annual PII and phishing training." P6 also used annual training but suggested that "quarterly training would also be beneficial." Training took place across different platforms. P1 and used online and classroom training, which included a cybersecurity specialist. P7 reported using both video courses and lectures, "Most training that are offered to customers are lectures and video courses." P8 explained, "The Workforce Development Team offers in-person digital literacy training," and customers are allowed to earn certificates and badges through more training online.

In addition to online and in-person training, other information was provided to users to help safeguard PII. P4 provided customers with pamphlets outlining standard phishing techniques and other kinds of threats to data. P5 gave clients "basic information about information security practices." Two participants found an effective way to educate users was to conduct exercises that showed the impact of a data breach. P3 stated, "[I use] phishing exercises using known attack vectors [to show] the impact it has on the organizational image if the attack is successful." Similarly, P6 said, "Users should be made aware of the consequences of falling victim to phishing attacks.

User awareness and training are the best defense against phishing attacks aligned with existing literature concerning user awareness and training as a strategy to defend against phishing attacks. Because users are the first line of defense in protecting data, they must be aware of the threats they may face and the tools to defend against them. According to the SBA (2019), employees opening malicious emails are among the primary causes of data breaches for small businesses. Nguyen and Kim (2017) asserted that when users have the knowledge and skills to protect information and information systems, they are likely to engage in appropriate security behavior. Pham et al. (2017) wrote that understanding the severity of a threat and the likelihood of it occurring may positively influence users' compliance behavior. In addition, Slonka and Shrift (2016) argued that presenting users with real phishing emails is an effective strategy to evaluate the impact of phishing on an organization's network.

The theme of user awareness and training is the best defense against phishing attacks aligned with TAM's PU and UTAUT's PE. PU refers to IT managers' belief that user awareness and training prevent phishing attacks. PE refers to user awareness training as an effective strategy to prevent phishing attacks. Ključnikov et al. (2019) and Flowerday and Tuyikeze (2016) observed that information security awareness, education, and senior management support were an information security program's most crucial success factors. Senior management involvement in information security awareness training ensures that adequate resources for maintaining the program are available. Likewise, Hwang et al. (2021) discovered that information security training, management participation, policies, and visible security positively impacted users' security awareness.

Molino et al. (2020) found a positive relationship between users' technology acceptance and training, information, and resilience. Enhancing the human element of cybersecurity is necessary for preventing cyberattacks. While it is impossible to prevent all cyberthreats, small businesses can make themselves less susceptible by investing in information security awareness and training. Information security awareness and training can improve employees' confidence in adopting and implementing appropriate security behavior.

Applications to Professional Practice

The specific IT problem that formed the basis of this research was that small businesses' IT managers lack strategies for preventing phishing attacks resulting in PII data breaches. Many small businesses do not have effective strategies to protect their customers' PII from phishing attacks. However, the IT managers that participated in this study implemented procedures to protect PII from phishing attacks. The eight participants have experience working in small businesses where personnel and financial resources are sometimes limited. Because of resource constraints, the participants needed cost-effective and straightforward strategies. The research results showed the importance of information security awareness and training, technology, and management support in implementing security strategies to protect PII. Small businesses will find this study helpful in identifying strategies that can help protect their customers' PII against phishing attacks. The results obtained from this data could help create guidelines or best practices for organizations to improve or enhance their current information security programs. The findings of this study may be valuable in professional practice by prompting IT managers to consider increasing their knowledge and understanding of effective information security strategies to prevent data breaches.

Implications for Social Change

Implications for positive social change include adding to the body of knowledge of strategies for IT Managers and organizations to protect customers' PII against phishing attacks. This study's findings may help IT managers develop effective strategies or frameworks for protecting their customers' PII from phishing attacks. There is also the potential to contribute new insights to help develop new procedures for small businesses to safeguard their data and information against theft or intrusions. Through improved information security strategies, small businesses may avoid the consequences of having their customers' PII compromised. More robust information security could also raise small business' customers' confidence in their ability to protect their personal and financial information. The public could benefit from this study's findings by offering information about protecting themselves from phishing attacks and preventing the loss or compromise of data.

Recommendations for Action

IT managers who lack strategies for preventing phishing attacks resulting in PII data breaches may use this study's results to develop an effective information security program. Information security awareness and training are essential aspects of an organization's information security program. IT managers can use the findings of this study to develop an information security checklist for their organizations. IT managers should strive to foster an environment that promotes acceptable security behavior and attitudes. Information security policies should be straightforward and easily accessible. IT managers should make information security training and awareness programs vital to their organizational cybersecurity policies. Information security training should be tailored to specific audiences as employees' threats may differ based on their positions. Employees are the first line of defense in information security; therefore, they must understand their roles and responsibilities in protecting their organization's data. Also, senior management should support information security by allocating funds and personnel. Without managerial and financial support, information security strategy implementation is challenging.

Compelling employees to comply with information security policies requires management's willingness to enforce those policies. Appropriating funds for information security is necessary to acquire, maintain, or upgrade the security infrastructure, execute security programs, user training, and policy enforcement. IT managers would benefit from conducting regular audits to review and update information security policies and training to ensure they are relevant to current security risks and threats. Senior leaders should communicate their expectations for updating and disseminating security policies, procedures, and training. Once the study is approved, I will share the literature results through conferences, scholarly journals, business journals, and training. Furthermore, I provided copies of the final research via email to all study participants.

Recommendations for Further Study

An effective information security program requires a combination of people, processes, and technology. While all elements are necessary for protecting data, it is the human element that the research participants emphasized. Employees and end-users are the first line of defense for protecting information and information systems. Therefore, users must receive the tools needed to protect themselves and their organizations from common phishing tactics. Processes are only effective when people adhere to them. Hence, management must be committed to fostering a security conscience environment. Technology is useful when it works as intended and is maintained and updated consistently. Thus, IT managers should ensure that information security software is patched regularly and upgraded when appropriate.

My recommendations for further research derive from the assumptions and limitations related to the research, literature, and information obtained from conducting interviews. One assumption of the study was that interview questions would produce rich, thick data to address the research question. Participants' responses to interview questions are based on their individual experiences. I recommend that additional qualitative research studies include organizations and different locations to determine whether the findings from new research would correspond to my findings. This study was limited because the results may not be generalizable to the small business population because of the small sample size. I recommend that additional research be conducted using a different design or method. A quantitative study could examine the correlation of the results across a more significant segment of the small business population. The findings from this study highlighted the importance of information security awareness and training. Further research into information security training and awareness will reduce the risks of users falling victim to phishing attacks. In the end, this study has contributed to the literature and paved the way for additional research in the information security industry.

Reflections

The doctoral research study was one of the most challenging academic endeavors I have ever experienced. Prior to starting my research, I did not realize the level of commitment required for completion. I spent many days, nights, and weekends reading, writing, and revising. I also encountered a few obstacles along the way; however, I always found a way to navigate them and move forward. Perseverance, discipline, and stamina were vital for completing my doctoral journey. Perseverance was needed to work through obstacles as they appeared. Discipline was required to continue writing instead of spending time with friends and family. Stamina helped me stay on course during a very long doctoral journey. At the same time, I am a better writer and researcher because of my doctoral research. I also better understood the qualitative research method and case study design. What is more, I had the opportunity to interview eight IT professionals who helped me understand the strategies small businesses use to protect data. As a result, I learned how to collect, analyze, and present data to help others transmit and store sensitive information safely and securely.

Summary and Study Conclusion

IT managers develop and implement information security strategies to protect data from theft, loss, or compromise. Creating an environment that is security conscience requires time, consistent information security awareness training, information security policies, technological solutions, and management support. Senior executive leadership must buy into information security implementation and provide support through appropriate funding and constant communication. The participating IT managers agree that a trained workforce is the first step towards reducing the risk of losing data through social engineering or phishing attacks. Small businesses can improve their overall security posture through information security technology, physical security, and information security policies.

References

Abbas, J., Mahmood, H. K., & Hussain, F. (2015). Information security management for small and medium size enterprises. *Science International-Lahore, 27*(3), 2393–2398.

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

Adhikar, K., & Panda, R. K. (2018). Users' information privacy concerns and privacy protection behaviors in social networks. *Journal of Global Marketing, 31*(2), 96–110. https://doi.org/10.1080/08911762.2017.1412552

Adil, M., Khan, R., & Ghani, M. A. N. U. (2020). Preventive techniques of phishing attacks in networks. In *2020 3rd International Conference on Advancements in Computational Sciences,* 1-8. IEEE.

Ajibade, P. (2018). Technology acceptance model limitations and criticisms: Exploring the practical applications and use in technology-related studies, mixed-method, and qualitative researches. *Library Philosophy & Practice*, Article 1941.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211.

Aldawood, H., & Skinner, G. (2019, May 8-9). *Challenges of implementing training and awareness programs targeting cyber security social engineering* [Paper presentation]. 2019 Cybersecurity and Cyberforensics Conference, Melbourne, Australia. https://doi.org/10.1109/CCC.2019.00004

Al-Jumaili, T. (2018). *Exploring the information security policies and practices required by small and medium-sized IT enterprises* (10975031). [Doctoral dissertation, Colorado Technical University]. ProQuest Dissertations Publishing.

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

Almubayedh, D., Khalis, M. A., Alazman, G., Alabdali, M., Al-Refai, R., & Nagy, N. (2018, April 25-26). *Security related issues in Saudi Arabia small organizations: A Saudi case study.* [Paper presentation]. 2018 21st Saudi Computer Society National Computer Conference, Riyadh, Saudi Arabia. https://doi.org/10.1109/NCG.2018.8593058

Alpi, K. M., & Evans, J. J. (2019). Distinguishing case study as a research method from case reports as a publication type. *Journal of the Medical Library Association*, *107*(1), 1–5. https://doi.org/10.5195/jmla.2019.615

Alshaikh, M., Maynard, S. B., Ahmad, A., & Chang, S. (2018, January 3-6). *An exploratory study of current information security training and awareness practices in organizations* [Paper presentation]. 51st Hawaii International Conference on System Sciences, Waikoloa Village, Hawaii. https://doi.org/10.24251/hicss.2018.635

Alzamil, Z. A. (2018). Information security practice in Saudi Arabia: Case study on Saudi organizations. *Information & Computer Security, 26*(5), 568–583.

https://doi.org/10.1108/ICS-01-2018-0006

Andrade, C. (2021). The inconvenient truth about convenience and purposive samples. *Indian Journal of Psychological Medicine, 43*(1), 86–88. https://doi.org/10.1177/0253717620977000

Angraini, A., & Okfalisa, R. A. (2019). Information security policy compliance: Systematic literature review. *Procedia Computer Science*, *161*, 1216–1224. https://doi.org/10.1016/j.procs.2019.11.235

Antunes, C. H., Dias, L., Dantas, G., Mathias, J., & Zamboni, L. (2016). An application of soft systems methodology in the evaluation of policies and incentive actions to promote technological innovations in the electricity sector. *Energy Procedia, 106*(4–5), 258–278. https://doi.org/10.1016/j.egypro.2016.12.121

Apuke, O. D. (2017). Quantitative research methods: A synopsis approach. *Kuwait Chapter of Arabian Journal of Business and Management Review, 6*(11), 40–47. https://doi.org/10.12816/0040336

Ayyagari, R., & Figueroa, N. (2017). Is seeing believing? Training users on information security: Evidence from Java applets. *Journal of Information Systems Education, 28*(2), 115–121.

Bayraktaroglu, S., Kahya, V., Atay, E., & Ilhan, H. (2019). Application of expanded technology acceptance model for enhancing the HRIS usage in SMEs. *International Journal of Applied Management & Technology*, *18*(1), 48–66. https://doi.org/10.5590/IJAMT.2019.18.1.04

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

Benoot, C., Hannes, K., & Bilsen, J. (2016). The use of purposeful sampling in a qualitative evidence synthesis: A worked example on sexual adjustment to a cancer trajectory. *BMC Medical Research Methodology, 16*(1), 21–25. https://doi.org/10.1186/s12874-016-0114-6

Berry, C. T., & Berry, R. L. (2018). An initial assessment of small business risk management approaches for cyber security threats. *International Journal of Business Continuity and Risk Management*, *8*(1), 1-10.

Bhardwaj, A., Sapra, V., Kumar, A., Kumar, N., & Arthi, S. (2020). Why is phishing still successful? *Computer Fraud & Security, 2020*(9), 15-19.

Bhardwaj, P. (2019). Types of sampling in research. *Journal of the Practice of Cardiovascular Sciences*, *5*(3), 157. https://doi.org/10.4103/jpcs.jpcs_62_19

Billingsley, L. (2019). Cybersmart: Protect the patient, protect the data. *Journal of Radiology Nursing*, *38*(4), 261–263. https://doi.org/10.1016/j.jradnu.2019.09.010

Billups, F. D. (2019). *Qualitative data collection tools: Design, development, and applications* (55). SAGE Publications.

Birt, L., Scott, S., Cavers, D., Campbell, C., & Walter, F. (2016). Member checking. *Qualitative Health Research, 26*(13), 1802-1811. https://doi.org/10.1177/1049732316654870

Bolek, V., Látečková, A., Romanová, A., & Korček, F. (2016). Factors affecting information security focused on SME and agricultural enterprises. *Agris on-line Papers in Economics and Informatics*, *8*(665-2016-45137), 37-50.

https://doi.org/10.7160/aol.2016.080404

Borowska-Beszta, B. (2017). Decoding of bias in qualitative research in disability cultures: A review and methodological analysis. *International Journal of Psycho-Educational Sciences*, *6*(3), 55–68.

Bu, F., Wang, N., Jiang, B., & Jiang, Q. (2021). Motivating information system engineers' acceptance of privacy by design in China: An extended UTAUT model. *International Journal of Information Management*, *60*. https://doi.org/10.1016/j.ijinfomgt.2021.102358

Campbell, S., Greenwood, M., Prior, S., Shearer, T., Walkem, K., Young, S., Bywaters, D., & Walker, K. (2020). Purposive sampling: complex or simple? Research case examples. *Journal of Research in Nursing*, *25*(8), 652-661. https://doi.org/10.1177/1744987120927206

Čančer, V., & Mulej, M. (2010). The dialectical systems theory's capacity for multi-criteria decision-making. *Systems Research & Behavioral Science, 27*(3), 285-300. https://doi.org/10.1002/sres.1016

Castiblanco Jimenez, I. A., Cepeda García, L. C., Violante, M. G., Marcolin, F., & Vezzetti, E. (2021). Commonly used external TAM variables in e-learning, agriculture, and virtual reality applications. *Future Internet*, 13. https://doi.org/10.3390/fi13010007

Castillo-Montoya, M. (2016). Preparing for interview research: The interview protocol refinement framework. *Qualitative Report*, *21*(5).

Castleberry, A., & Nolen, A. (2018). Thematic analysis of qualitative research data: Is it as easy as it sounds? *Currents in Pharmacy Teaching and Learning, 10*(6), 807-815. https://doi.org/10.1016/j.cptl.2018.03.019

Checkland, P. (2012). Four conditions for serious systems thinking and action. *Systems Research and Behavioral Science, 29*(5), 465-469. https://doi.org/10.1002/sres.2158

Chinyemba, M. K., & Phiri, J. (2018). An investigation into information security threats from insiders and how to mitigate them: A case study of Zambian public sector. *Journal of Computer Science, 14*(10), 1389-1400. https://doi.org/10.3844/jcssp.2018.1389.1400

Choi, S., Martins, J. T., & Bernik, I. (2018). Information security: Listening to the perspective of organisational insiders. *Journal of Information Science, 44*(6), 752-767. https://doi.org/10.1177/0165551517748288

Chul, W. Y., Goo, J., & Rao, H. R. (2020). Is cybersecurity a team sport? A multilevel examination of workgroup information security effectiveness. *MIS Quarterly, 44*(2), 907-931. https://doi.org/10.25300/MISQ/2020/15477

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

Connelly, L. M. (2016). Trustworthiness in qualitative research. *Medsurg Nursing, 25*(6), 435. https://www.ncbi.nlm.nih.gov/pubmed/30304614

Cuganesan, S., Steele, C., & Hart, A. (2018). How senior management and workplace norms influence information security attitudes and self-efficacy.

Cypress, B. S. (2017). Rigor or reliability and validity in qualitative research:

Perspectives, strategies, reconceptualization, and recommendations. *Dimensions of Critical Care Nursing, 36*(4), 253-263. https://doi.org/10.1097/DCC.0000000000000253

Daniel, B. K. (2019). Using the TACT framework to learn the principles of rigour in qualitative research. *Electronic Journal of Business Research Methods, 17*(3), 118-129. https://doi.org/10.34190/JBRM.17.3.002

Das, S., Kim, A., Tingle, Z., & Nippert-Eng, C. (2019). All about phishing: Exploring user research through a systematic literature review. ArXiv preprint. arXiv:1908.05897.

Davis, F. D. (1986). A technology acceptance model for empirically testing new end-user information systems. [Doctoral dissertation]. Cambridge, MA.

Davis, F. D. (1989). Perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319–340. https://doi.org/10.2307/249008

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, *35*(8), 982.

Diesch, R., & Krcmar, H. (2020). SoK: Linking information security metrics to management success factors. *Proceedings of the 15th International Conference on Availability, Reliability and Security,* 1-10. https://doi.org/10.1145/3407023.3407059

Dombora, S. (2019). Parameters and guidelines of enforceable information security management systems. *Interdisciplinary Description of Complex Systems 17*(3-A), 485-491. https://doi.org/10.7906/indecs.17.3.7

Doyle, L., Brady, A. M., & Byrne, G. (2009). An overview of mixed methods research. *Journal of research in nursing*, *14*(2), 175-185.

Dube, E., & Flowerday, S. (2018). Towards a holistic information security framework for South African small and medium enterprises. *2018 1st International Conference on Computer Applications & Information Security.* [Paper presentation]. 1-4. https://doi.org/10.1109/CAIS.2018.8442018

Edmonds, E. A. (2017). General system theory: Foundations, development, applications by Ludwig Von Bertalanffy (review). *Leonardo, 10*(3), 248.

Elliott, V. (2018). Thinking about the coding process in qualitative data analysis. *The Qualitative Report, 23*(11), 2850-2861. https://www.proquest.com/scholarly-journals/thinking-about-coding-process-qualitative-data/docview/2155621346/se-2?accountid=45205

Ellis, P. (2019). The language of research (part 20): Understanding the quality of a qualitative paper (2). *Wounds UK, 15*(1), 110-111.

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American journal of theoretical and applied statistics*, *5*(1), 1-4.

Fathi, M. R., Maleki, M. H., Sobhani, S. M., & Koksal, C. D. (2020). Future study of operations research based on scenario planning and soft systems methodology. *Foresight*.

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

Fishbein, M., & Ajzen, I. (1977). Belief, attitude, intention, and behavior: An introduction to theory and research. *Philosophy and Rhetoric*, *10*(2).

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

Flowerday, S. V., & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. *Computers & Security, 61*, 169-183. https://doi.org/10.1016/j.cose.2016.06.002

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

Fusch, P., Fusch, G. E., & Ness, L. R. (2018). Denzin's paradigm shift: Revisiting triangulation in qualitative research. *Journal of Social Change, 10*(1). https://doi.org/10.5590/JOSC.2018.10.1.02

Gafni, R., & Patel, T. (2019). The invisible hole of information on SMB's cybersecurity *Online Journal of Applied Knowledge Management, 7(1).*

Garone, A., Pynoo, B., Tondeur, J., Cocquyt, C., Vanslambrouck, S., Bruggeman, B., & Struyven, K. (2019). Clustering university teaching staff through UTAUT: Implications for the acceptance of a new learning management system. *British*

Journal of Educational Technology, *50*(5), 2466-2483.

Gerring, J. (2017). Qualitative methods. *Annual Review of Political Science, 20*(1), 15-36. https://doi.org/10.1146/annurev-polisci-092415-024158

Goertzen, M. J. (2017). Introduction to quantitative research and data. *Library Technology Reports, 53*(4), 12-18. https://search.proquest.com/docview/1903876597

Grannemann, J. (2018). The business guide to improving information security. *The Journal of Equipment Lease Financing (Online), 36*(3), 1-9. https://search.proquest.com/docview/2155627198

Gunawan, H., Sinaga, B. L., & WP, S. P. (2019). Assessment of the readiness of micro, small and medium enterprises in using e-money using the unified theory of acceptance and use of technology (UTAUT) method. *Procedia Computer Science*, *161*, 316–323. https://doi.org/10.1016/j.procs.2019.11.129

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

Hancock, D. R., & Algozzine, B. (2017). *Doing case study research: A practical guide for beginning researchers.* Teachers College Press.

Haqaf, H., & Koyuncu, M. (2018). Understanding key skills for information security managers. *International Journal of Information Management*, *43*, 165–172. https://doi.org/10.1016/j.ijinfomgt.2018.07.013

Harris, K. (2016). Attorney General California Department of Justice. *California data* *breach report 2012-2015*. https://www.oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf

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

Hasbini, M. A., Eldabi, T., & Aldallal, A. (2018). Investigating the information security management role in smart city organisations. *World Journal of Entrepreneurship, Management and Sustainable Development*.

Hayes, M. T., Sameshima, P., & Watson, F. (2015). Imagination as Method. *International Journal of Qualitative Methods*, *14*(1), 36–52. https://doi.org/10.1177/160940691501400105

Herath, T., Yim, Y. S., D'Arcy, J., Nam, K., & Rao, H. R. (2018). Examining employee security violations: Moral disengagement and its environmental influences. *Information Technology & People, 31*(6), 1135-1162. https://doi.org/10.1108/ITP-10-2017-0322

Hesse-Biber, S. (2020). Taking public action on private troubles: The power of hybrid methodology mixed methods research in the public sphere. *Qualitative Inquiry, 26*(2), 153-164. https://doi.org/10.1177/1077800419857755

Hofkirchner, W. (2019). Social relations: Building on Ludwig Von Bertalanffy. *Systems Research & Behavioral Science, 36*(3), 263-273. https://doi.org/10.1002/sres.2594

Hwang, I., Wakefield, R., Kim, S., & Kim, T. (2021). Security awareness: The first step in information security compliance behavior. *Journal of Computer Information Systems*, *61*(4), 345-356.

Ionescu, R. C., Ceaușu, I., & Ilie, C. (2018). Considerations on the implementation steps for an information security management system. *Proceedings of the International Conference on Business Excellence, 12*(1), 476-485. https://doi.org/10.2478/picbe-2018-0043

Iyamuremye, B., & Shima, H. (2018). Network security testing tools for SMEs (small and medium enterprises). *IEEE International Conference on Applied System Invention,* 414-417. IEEE.

Jalali, M. F. M., & Heidari, H. (2020). Predicting changes in bitcoin price using grey system theory. *Financial Innovation, 6*(1), 1-12.

Javed, S. A., & Liu, S. (2017). Evaluation of project management knowledge areas using grey incidence model and AHP. *2017 International Conference on Grey Systems and Intelligent Services.* [Paper presentation]. 120.

Jones, J., & Smith, J. (2017). Ethnography: challenges and opportunities. https://doi.org/10.1136/eb-2017-102786

Jordan, K. (2018). Validity, reliability, and the case for participant-centered research: Reflections on a multi-platform social media study. *International Journal of Human-Computer Interaction, 34*(10), 913-921. https://doi.org/10.1080/10447318.2018.1471570

Ki-Aries, D., & Faily, S. (2017). Persona-centered information security awareness. *Computers & Security*, *70*, 663–674.

https://doi.org/10.1016/j.cose.2017.08.001

Kim, H., Sefcik, J. S., & Bradway, C. (2017). Characteristics of qualitative descriptive studies: A systematic review. *Research in Nursing & Health, 40*(1), 23-42. https://doi.org/10.1002/nur.21768

Ključnikov, A., Mura, L., & Sklenár, D. (2019). Information security management in SMEs: Factors of success. *Entrepreneurship and Sustainability Issues, 6*(4), 2081-2094. https://doi.org/10.9770/jesi.2019.6.4(37)

Lambert, V. A., & Lambert, C. E. (2012). Qualitative descriptive research: An acceptable design. *Pacific Rim International Journal of Nursing Research, 16*(4), 255-256.

Legg, P., & Blackman, T. (2019). Tools and techniques for improving cyber situational awareness of targeted phishing attacks. In 2019 *International Conference on Cyber Situational Awareness, Data Analytics and Assessment,*1-4. IEEE.

Lemon, L. (2017). Applying a mindfulness practice to qualitative data collection. *Qualitative Report, 22*(12), 3305.

Levitt, H. M., Bamberg, M., Creswell, J. W., Frost, D. M., Josselson, R., & Suárez-Orozco, C. (2018). Journal article reporting standards for qualitative primary, qualitative meta-analytic, and mixed methods research in psychology: The APA publications and communications board task force report. *The American Psychologist, 73*(1), 26-46. https://doi.org/10.1037/amp0000151

Lin, C. S. (2017). Revealing the “essence” of things: Using phenomenology in LIS research. *Qualitative and Quantitative Methods in Libraries, 2*(4), 469-478.

Lin, H. C., & Chang, C. M. (2018). What motivates health information exchange in social media? The roles of the social cognitive theory and perceived interactivity. *Information & Management, 55*(6), 771-780.

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

Liu, S., Lin, C., & Yang, Y. (2017). Several problems need to be studied in grey system theory. *International Conference on Grey Systems and Intelligent Services* (GSIS), 1-4. https://doi.org/10.1109/GSIS.2017.8077658.

Lopes, I. M., & Oliveira, P. (2016). Adoption of an information systems security policy in small and medium sized enterprises. *Journal of Information Systems Engineering & Management, 1*(1). https://doi.org/10.20897/lectito.201605

Mackieson, P., Shlonsky, A., & Connolly, M. (2019). Increasing rigor and reducing bias in qualitative research: A document analysis of parliamentary debates using applied thematic analysis. *Qualitative Social Work: Research and Practice*, *18*(6), 965–980. https://doi.org/10.1177/1473325018786996

Magilvy, J. K., & Thomas, E. (2009). A first qualitative project: Qualitative descriptive design for novice researchers. *Journal for Specialists in Pediatric Nursing, 14*(4), 298-300. https://doi.org/10.1111/j.1744-6155.2009.00212.x

Maxwell, J. A. (2020). Why qualitative methods are necessary for generalization. *Qualitative Psychology,* Washington, D.C. https://doi.org/10.1037/qup0000173

McClelland, S. I. (2017). Vulnerable listening: Possibilities and challenges of doing qualitative research. *Qualitative Psychology, 4*(3), 338-352. Washington, D.C*.,* https://doi.org/10.1037/qup0000068

McLaughlin, M. D., & Gogan, J. (2018). Challenges and best practices in information security management. *MIS Quarterly Executive*, *17*(3), 12.

Mierzwiak, R., Xie, N., & Dong, W. (2019). Classification of Research Problems in Grey System Theory based on Grey Space Concept. *Journal of Grey System*, *31*(1).

Mohajan, H. K. (2017). Two criteria for good measurements in research: Validity and reliability. *Annals of Spiru Haret University. Economic Series, 17*(4), 59-82. https://doi.org/10.26458/1746

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

Mohamad, M. A., Radzi, S. M., & Hanafiah, M. H. (2021). Understanding tourist mobile hotel booking behaviour: Incorporating perceived enjoyment and perceived price value in the modified technology acceptance model. *Tourism & Management Studies*, *17*(1), 19–30. https://doi.org/10.18089/tms.2021.170102

Mohammad-Salehi, B., Vaez-Dalili, M., & Tabrizi, H. H. (2021). Investigating factors that influence EFL teachers' adoption of web 2.0 technologies: Evidence from Applying the UTAUT and TPACK. *TESL-EJ*, *25*(1), 1–21.

Molino, M., Cortese, C. G., & Ghislieri, C. (2020). The promotion of technology acceptance and work engagement in industry 4.0: From personal resources to information and training. *International journal of environmental research and public health*, *17*(7), 2438.

Moon, M. D. (2019). Triangulation: A method to increase validity, reliability, and legitimation in clinical research. *Journal of Emergency Nursing, 45*(1), 103-105. https://doi.org/10.1016/j.jen.2018.11.004

Moser, A., & Korstjens, I. (2017). Series: Practical guidance to qualitative research. Part 3: Sampling, data collection and analysis. *The European Journal of General Practice, 24*(1), 9-18. https://doi.org/10.1080/13814788.2017.1375091

Murshed, F., & Zhang, Y. (2016). Thinking orientation and preference for research methodology. *Journal of Consumer Marketing, 33*(6), 437–446. https://doi.org/10.1108/JCM-01-2016-1694

Mushi, R. M. (2018). The impact of personal privacy on the acceptance of mobile phone technology: A case of Tanzanian SMEs. *Journal of International Technology and Information Management, 27*(1), 129-144.

Naderifar, M., Goli, H., & Ghaljaie, F. (2017). Snowball sampling: A purposeful method of sampling in qualitative research. *Strides in Development of Medical Education, 14*(3), 1-6. https://doi.org/10.5812/sdme.67670

National Institutes of Health. (1979). The Belmont Report. *Belmont Report Ethical Principals and Guidelines for the Protection of Human Subjects of Research*, 4-6.

Nguyen, Q. N., & Kim, D. J. (2017). Enforcing information security protection: Risk propensity and self-efficacy perspectives. In *Proceedings of the 50th Hawaii International Conference on System Sciences*.

Njenga, K., & Jordaan, P. (2016). We want to do it our way: The neutralisation approach to managing information systems security by small businesses. *The African Journal of Information*

Systems, 8(1). https://digitalcommons.kennesaw.edu/ajis/vol8/iss1/3/

Nowak, M., Mierzwiak, R., & Butlewski, M. (2020). Occupational risk assessment with grey system theory. *Central European Journal of Operations Research, 28*(2), 717-732.

O'Kane, P., Smith, A., & Lerman, M. P. (2021). Building transparency and trustworthiness in inductive research through computer-aided qualitative data analysis software. *Organizational Research Methods*, *24*(1), 104–139. https://doi.org/10.1177/1094428119865016

Owen-Smith, A., & Coast, J. (2017). Understanding sampling and recruitment. *Qualitative Methods in Health Economics.,* 42-58.

Pagura, I. (2019). Small business and cybersecurity*. Journal of the Australian Traditional-Medicine Society*, *26*(1), 38–39.

Panjwani, M., Jantti, M., & Sormunen, J. (2016). IT service management from a perspective of small and medium sized companies. *2016 10th International Conference on the Quality of Information and Communications Technology,* 210-215. https://doi.org/10.1109/QUATIC.2016.053

Park, J., & Park, M. (2016). Qualitative versus quantitative research methods: Discovery or justification? *Journal of Marketing Thought*, *3*(1), 1–7.

Paulsen, C., & Toth, P. (2016). *Small business information security: The fundamentals.* (NISTIR 7621 Revision 1 ed.). National Institute of Standards and Technology (NIST), U.S. Department of Commerce. https://doi.org/10.6028/nist.ir.7621r1

Pereira, C. (2020). Security and regulatory factors impact on the adoption of cloud computing by IT managers: A correlational study (27995993). [Doctoral Dissertation, Capella University] ProQuest Dissertations Publishing.

Peterson, F., Jacobs, M., & Pather, S. (2020). Barriers for user acceptance of mobile health applications for diabetic patients: Applying the UTAUT model. https://doi.org/10.1007/978-3-030-45002-1_6

Pham, H., Brennan, L., & Richardson, J. (2017). Review of behavioural theories in security compliance and research challenge. In *Informing Science and Information Technology Education Conference, Vietnam*, 65-76.

Phillips, R., & Tanner, B. (2019). Breaking down silos between business continuity and cyber security. *Journal of Business Continuity & Emergency Planning, 12*(3), 224-232. http://openurl.ingenta.com/content?genre=article&issn=1749-9216&volume=12&issue=3&spage=224&epage=232

Popescul, D. (2018). Information security awareness in contemporary organizations – challenges and solutions. *Security & Future, 2*(3), 134–137. https://stumejournals.com/journals/confsec/2018/3/134.full.pdf

Prislan, K., Lobnikar, B., & Bernik, I. (2017). Information security management practices: Expectations and reality. *Advances in Cybersecurity 2017, 2017*, 5-22. https://doi.org/10.18690/978-961-286-114-8.1

Pruitt, D. A. (2019). Security factors influencing the adoption of cloud computing by decision making it managers (22621879). [Doctoral Dissertation, Sullivan University]. ProQuest Dissertations Publishing.

Puriwat, W., & Tripopsakul, S. (2021). Explaining social media adoption for a business purpose: An application of the UTAUT model. *Sustainability*, *13*(2082), 2082. https://doi.org/10.3390/su13042082

Ramadania, S., & Braridwan, Z. (2019). The influence of PU, ease of use, attitude, self-efficacy, and subjective norms toward intention to use online shopping. *International Business and Accounting Research Journal*, *3*(1), 1–14. https://doi.org/10.15294/ibarj.v3i1.45

Ramsey, F., & Seyyedhasani, H. (2021). Cyber attacks in agriculture: Protecting your farm and small business with cyberbiosecurity.

Rao, S. S., & Liu, X. T. (2017). Universal grey system theory for analysis of uncertain structural systems. *AIAA Journal, 55*(11), 3966-3979.

Razaque, A., Amsaad, F., Hariri, S., Almasri, M., Rizvi, S. S., & Frej, M. B. H. (2020). Enhanced grey risk assessment model for support of cloud service provider. *IEEE Access*, *8*, 80812-80826.

Razmak, J., & Bélanger, C. (2018). Using the technology acceptance model to predict patient attitude toward personal health records in regional communities. *Information Technology & People*, *31*(2), 306–326. https://doi.org/10.1108/ITP-07-2016-0160

Reyes-Mercado, P., & Barajas-Portas, K. (2020). Analysis of the usage intensity of digital advertising platforms by SMEs using an integrated models. *Journal of Business-to-Business Marketing*, *27*(4), 407–417. https://doi.org/10.1080/1051712X.2020.1831215

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

Ritz, W., Wolf, M., & McQuitty, S. (2019). Digital marketing adoption and success for small businesses: The application of the do-it-yourself and technology acceptance models. *Journal of Research in Interactive Marketing*, *13*(2), 179–203. https://doi.org/10.1108/JRIM-04-2018-0062

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

Rosenthal, M. (2016). Qualitative research methods: Why, when, and how to conduct interviews and focus groups in pharmacy research. *Currents in Pharmacy Teaching and Learning, 8*(4), 509-516. https://doi.org/10.1016/j.cptl.2016.03.021

Rostami, E., Karlsson, F., & Gao, S. (2020). Requirements for computerized tools to design information security policies. *Computers & Security, 99.* https://doi.org/10.1016/j.cose.2020.102063

Rozmi, A. N. A., Bakar, M. I. A., Hadi, A. R. A., & Nordin, A. I. (2019). Investigating the intentions to adopt ICT in Malaysian SMEs using the UTAUT Model. In *International Visual Informatics Conference*, 477-487. Springer, Cham

Rutberg, S., & Bouikidis, C. D. (2018). Focusing on the fundamentals: A simplistic differentiation between qualitative and quantitative research. *Nephrology Nursing Journal: Journal of the American Nephrology Nurses' Association, 45*(2), 209-213. https://www.ncbi.nlm.nih.gov/pubmed/30303640

Sadiq, A., Anwar, M., Butt, R. A., Masud, F., Shahzad, M. K., Naseem, S., & Younas, M. (2021). A review of phishing attacks and countermeasures for Internet of things-based smart business applications in industry 4.0. *Human Behavior and Emerging Technologies.*

Sadok, M., & Bednar, P. (2016). Information security management in SMEs: Beyond the IT challenges. In *Proceedings of the Tenth International Symposium on Human Aspects of Information Security & Assurance*, 209-219.

Sahin, F., Sen, M., & Dincer, C. (2019). Early childhood preservice teachers' experiences with reflective journal writing. *Eurasian Journal of Educational Research, 84*, 93–114. https://doi.org/10.14689/ejer.2019.84.5

Saldaña, J. (2015). *The coding manual for qualitative researchers*. Sage.

Saroia, A. I., & Gao, S. (2019). Investigating university students' intention to use mobile learning management systems in Sweden. *Innovations in Education and Teaching International, 56*(5), 569-580. https://doi.org/10.1080/14703297.2018.1557068

Savela, T. (2018). The advantages and disadvantages of quantitative methods in schoolscape research. *Linguistics and Education, 44*, 31-44. https://doi.org/10.1016/j.linged.2017.09.004

Schoonenboom, J. (2018). Designing mixed methods research by mixing and merging methodologies: A 13-step model. *American Behavioral Scientist, 62*(7), 998-1015. https://doi.org/10.1177/0002764218772674

Selznick, L., & LaMacchia, C. (2018). Cybersecurity liability: How technically savvy can we expect small business owners to be? *Journal of Business & Technology Law,* *13*(2), 217. https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?referer=https://scholar.google.com/&httpsredir=1&article=1289&context=jbtl

Sengkhyavong, W. S. (2019). Factors relating to the adoption of cloud computing by IT managers: A correlational study (13899358). [Doctoral dissertation, Capella University] ProQuest Dissertations Publishing.

Setia, M. S. (2017). Methodology series module 10: Qualitative health research. *Indian Journal of Dermatology, 62*(4), 367-370. https://doi.org/10.4103/ijd.IJD_290_17

Sharma, R., Zhang, C., Wingreen, S. C., Kshetri, N., & Zahid, A. (2019). Design of blockchain-based precision health-care using soft systems methodology. *Industrial Management & Data Systems, 120*(3), 608-632. https://doi.org/10.1108/IMDS-07-2019-0401

Shih, H.-P. (2004). Extended technology acceptance model of Internet utilization behavior. *Information & Management*, *41*(6), 719. https://doi.org/10.1016/j.im.2003.08.009

Sikora, M., Dzieża, G., & Jasiński, M. (2017). Data safety audit in small and medium-sized enterprises - Case Study. *Studies & Proceedings of Polish Association for Knowledge Management*, *86*, 68–76.

Singh, A. N., & Gupta, M. P. (2017). Information security management practices: Case studies from India. *Global Business Review, 20*(1), 253-271. https://doi.org/10.1177/0972150917721836

Slonka, K., & Shrift, B. (2016). Phishing our clients: A step toward improving training via social engineering. *Issues in Information Systems, 17*(1), 231.

Small Business Administration. (2019). *Introduction to cybersecurity.* Small Business Administration. https://www.sba.gov/managing-business/cybersecurity/introduction-cybersecurity

Sondakh, J. J. (2017). Behavioral intention to use e-tax service system: An application of technology acceptance model. *European Research Studies*, *20*(2A), 48–64.

Soni, V., Anand, R., Dey, P. K., Dash, A. P., & Banwet, D. K. (2017). Digitizing grey portions of e-governance. *Transforming Government: People, Process and Policy, 11*(3), pp.419-455. https://doi.org/10.1108/TG-11-2016-0076

Sosin, A. (2018). How to increase the information assurance in the information age. *Journal of Defense Resources Management, 9*(1), 45-57. http://www.jodrm.eu

Sprenger, D. A., & Schwaninger, A. (2021). Technology acceptance of four digital learning technologies (classroom response system, classroom chat, e-lectures, and mobile virtual reality) after three months' usage. *International Journal of Educational Technology in Higher Education*, *18*(1), 1–17. https://doi.org/10.1186/s41239-021-00243-4

Susanty, A., Handoko, A., & Puspitasari, N. B. (2020). Push-pull-mooring framework for e-commerce adoption in small and medium enterprises. *Journal of Enterprise Information Management*, *33*(2), 381–406.

Sutoyo, M. A. H., & Sensuse, D. I. (2018). Designing a conceptual model for rice information systems using gamification and soft system methodology. *2018*

International Conference on Advanced Computer Science and Information Systems. [Paper presentation]. 63-68. https://doi.org/10.1109/ICACSIS.2018.8618195

Tai, J., & Ajjawi, R. (2016). Undertaking and reporting qualitative research. *Clinical Teacher*, *13*(3), 175–182. https://doi.org/10.1111/tct.12552

Theofanidis, D., & Fountouki, A. (2018). Limitations and delimitations in the research process. *Perioperative nursing*, *7*(3), 155-163.

Thompson, R. S. (2016). Cybersecurity: Getting proactive about data vulnerability. *Florida Bar Journal*, *90*(1), 36–37.

To, A. T., & Trinh, T. H. M. (2021). Understanding behavioral intention to use mobile wallets in Vietnam: Extending the TAM model with trust and enjoyment. *Cogent Business & Management, 8*(1), 1891661.

Torres, D. (2018). Cyber security and cyber defense for Venezuela: An approach from the soft systems methodology. *Complex & Intelligent Systems, 4*(3), 213.

Tschakert, K. F., & Ngamsuriyaroj, S. (2019). Effectiveness of and user preferences for security awareness training methodologies. *Heliyon, 5*(6), e02010. https://doi.org/10.1016/j.heliyon.2019.e02010

Vanderstraeten, R. (2019). Systems everywhere? *Systems Research & Behavioral Science, 36*(3), 255-262. https://doi.org/10.1002/sres.2596

Varma, A. (2018). Mobile banking choices of entrepreneurs: A unified theory of acceptance and use of technology (UTAUT) perspective. *Theoretical Economics Letters*, *8*(14), 2921. https://doi.org/10.4236/tel.2018.814183

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, *27*(3), 425–478. https://doi.org/10.2307/30036540

Von Bertalanffy, L. (1972). The history and status of general systems theory. *Academy of Management Journal, 15(*4), 407–426. https://doi.org/10.2307/255139

Waldkirch, M. (2020). Non-family CEOs in family firms: Spotting gaps and challenging assumptions for a future research agenda. *Journal of Family Business Strategy, 11*(1), 100305. https://doi.org/10.1016/j.jfbs.2019.100305

Wang, Y., Wang, S., Wang, J., Wei, J., & Wang, C. (2020). An empirical study of consumers' intention to use ride-sharing services: using an extended technology acceptance model. *Transportation*, *47*(1), 397-415. https://doi.org/10.1007/s11116-018-9893-4

Warren, S., Sauser, B., & Nowicki, D. (2019). A bibliographic and visual exploration of the historic impact of soft systems methodology on academic research and theory. *Systems, 7*(1), 10. https://doi.org/10.3390/systems7010010

Watad, M., Washah, S., & Perez, C. (2018). IT security threats and challenges for small firms: Managers' perceptions. *International Journal of the Academic Business World, 12*(1), 23–30.

Weis, D., & Willems, H. (2017). Aggregation, validation, and generalization of qualitative data - methodological and practical research strategies illustrated by the research process of an empirically based typology. *Integrative Psychological & Behavioral Science, 51*(2), 223-243. https://doi.org/10.1007/s12124-016-9372-

4

Wenham, P. (2016). Extra care needed. *ITNow, 58*(4), 22-23. https://doi.org/10.1093/itnow/bww098

Williams, B. (2018). How can adblocking play a significant role in an SME's defence strategy? *Computer Fraud & Security, 2018*(9), 18-20. https://doi.org/10.1016/S1361-3723(18)30089-7

Wolf, F., Aviv, A. J., & Kuber, R. (n.d.). *Security Obstacles and Motivations for Small Businesses from a CISO's Perspective*. 19.

Wu, Y. P., Thompson, D., Aroian, K. J., McQuaid, E. L., & Deatrick, J. A. (2016). Commentary: Writing and evaluating qualitative research reports. *Journal of Pediatric Psychology, 41*(5), 493-505. https://doi.org/10.1093/jpepsy/jsw032

Yin, R. K. (2013). Validity and generalization in future case study evaluations. *Evaluation*, *19*(3), 321-332.

Yoo, C. W., Goo, J., & Rao, H. R. (2020). Is cybersecurity a team sport? A multilevel examination of workgroup information security effectiveness. *MIS Quarterly*, *44*(2).

Zabukovšek, S. S., Bharadwaj, S. S., Bobek, S., & Štrukelj, T. (2019). Technology acceptance model-based research on differences of enterprise resources planning systems use in India and the European Union. *Engineering Economics*, *30* (3), 326–338. https://doi.org/10.5755/j01.ee.30.3.21211

Zain, F. M., Hanafi, E., Don, Y., Mohd Yaakob, M. F., & Sailin, S. N. (2019). Investigating student's acceptance of an EDMODO content management system. *International Journal of Instruction*, *12*(4), 1–16. https://doi.org/10.29333/iji.2019.1241a

Zammani, M., & Razali, R. (2016). An empirical study of information security management success factors. *International Journal on Advanced Science, Engineering, and Information Technology, 6*(6), 904. https://doi.org/10.18517/ijaseit.6.6.1371

Zayed, K. (2016). Information security awareness: Managing web, mobile & endpoint security; overcoming the challenges of bring your own device (BYOD). *International Journal of Teaching and Case Studies, 7*(3/4), 1. https://doi.org/10.1504/IJTCS.2016.10001478

Ženko, Z., Mulej, M., & Potočan, V. (2017). Knowledge-cum-values management belongs to the way out from global crisis. *Business Systems Research, 8*(1), 113-123. https://doi.org/10.1515/bsrj-2017-0009

Zenko, Z., Rosi, B., Mulej, M., Mlakar, T., & Mulej, N. (2012). Mulej's dialectical systems theory — A proven next step after Bertalanffy's general systems theory. *2012 IEEE International Conference on Complex Systems Complex Systems,* 1-8. https://doi.org/10.1109/ICoCS.2012.6458598

Appendix A: Letter of Invitation

Date: XX XXX XXXX

Dear Potential Research Participant,

My name is Erin Banks. Currently, I am an Information Technology doctoral student at Walden University. I invite you to participate in my doctoral research study entitled “Exploring Security Strategies to Protect Personally Identifiable Information in Small Businesses”. The information that will be collected during the study will be used to identify strategies in protecting the confidentiality, integrity, and availability of data to prevent data breaches. As the principal researcher for the study, I will interview participants who have experience dealing with information security. If you do not have such experience, please disregard this invitation.

The initial interview will be via Zoom or Skype and will take 30-60 minutes. We will schedule a follow-up interview to verify my understanding of your answers in the first interview, it is anticipated to take no more than 30 minutes.

For the study, participation is entirely voluntary. If you agree to partake in the study, you can decline participation at any time, or you may refuse to answer any questions that you do not wish to answer.

Information from the interview will be stored on an external hard drive and locked in a cabinet only accessible by me. Data from this study will be destroyed after 5 years from the date of completion of the final study. The results of this study will be published; however, your name and any identifying information will be removed from the data to protect your confidentiality.

There will be no payment for participation during the study.

The attached informed consent form will provide more details and will explain your rights in the study. If you agree to participate, please respond to this email with “I consent.”

Please provide a few specific times that would be convenient for the initial interview.

All your effort and time in participating in the study is greatly appreciated.

Sincerely,

Erin Banks

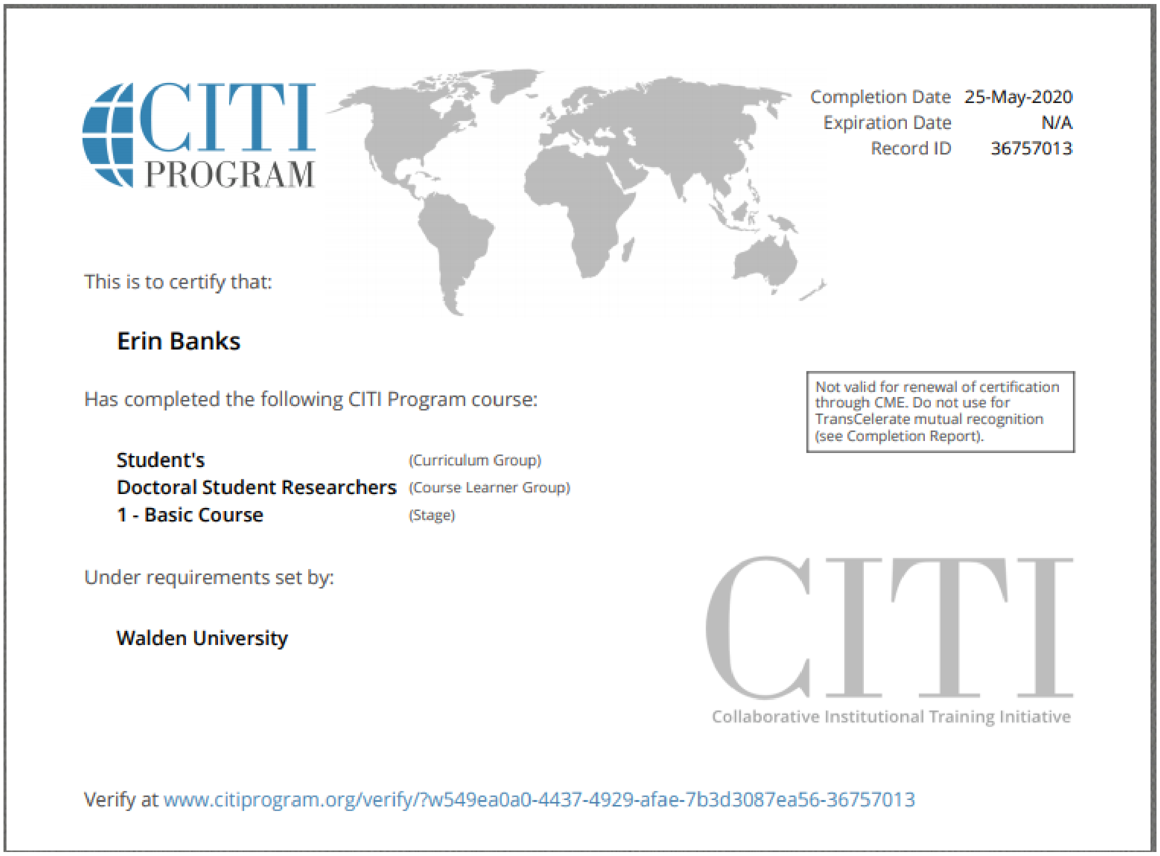
Appendix B: Interview Protocol

1. I will introduce myself to the participant, explain my role at Walden University and in the Information Technology field.
2. I will discuss with the participant during the interview that audio will be used to record them.
3. I will turn on the recording devices. Two records will be used as a failsafe.
4. I will discuss the confidentiality of the information.
5. I will review the conditions of the informed consent to which the participant previously consented by email.
6. I will begin the interview by asking about their background information.
7. I will discuss the purpose of the study.
8. I will be using the interview questions, as shown in Appendix B.
9. I will ask for their company's documents for security strategies after the interview.
10. I will explain to the participant that the interview will be transcribed and summarized, and a follow-up interview will be scheduled to verify the summarization of the interview transcript. We will set a time for the follow-up interview.
11. Audio recorders will be turned off before leaving.
12. When the interview is finished, I will thank the participant for their time and participation.

Appendix C: Interview Questions

1. What types of phishing attacks against customers' PII has your business experienced?
2. How do you protect your customers' PII against phishing attacks?
3. What are the considerations involved when developing strategies for protecting your customer's PII against phishing attacks?
4. What techniques have you found most effective in protecting your customers' PII against phishing attacks?
5. What is the challenges relative to the strategies used in protecting your customers' PII phishing attacks?
6. What types of training are offered to customers to protect their PII against phishing attacks?
7. What additional information about your experiences protecting your customers' PII against phishing attacks would you like to share?

Appendix D: Ethics Certificate



CITI PROGRAM

Completion Date	25-May-2020
Expiration Date	N/A
Record ID	36757013

This is to certify that:

Erin Banks

Has completed the following CITI Program course:

Not valid for renewal of certification through CME. Do not use for TransCelerate mutual recognition (see Completion Report).

Student's	(Curriculum Group)
Doctoral Student Researchers	(Course Learner Group)
1 - Basic Course	(Stage)

Under requirements set by:

Walden University

CITI
Collaborative Institutional Training Initiative

Verify at www.citiprogram.org/verify/?w549ea0a0-4437-4929-afae-7b3d3087ea56-36757013

Appendix E: Participant Demographics

	Age			Years of infosec experience		
Gender	35-40	41-50	51-60	2-5	6-10	11+
Male	2	3	2	1	1	5
Female			1		1	