2020

Maintaining Small Retail Business Profitability by Reducing Cyberattacks

Ira Johnson Phillips
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Ira J. Phillips, Jr.

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. Alexandre Lazo, Committee Chairperson, Doctor of Business Administration Faculty

Dr. Janet Booker, Committee Member, Doctor of Business Administration Faculty

Dr. Ronald Jones, University Reviewer, Doctor of Business Administration Faculty

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

Walden University
2020

Abstract

Maintaining Small Retail Business Profitability by Reducing Cyberattacks

by

Ira J. Phillips, Jr.

MA, American Military University, 2015

BS, Faulkner University, 1998

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

June 2020

Abstract

Ineffective cybersecurity strategies can detrimentally impact business profits. Small business owners who face challenges in remaining profitable because of increased cyberattacks on their business are at risk of failure. Grounded in general systems theory, the purpose of this qualitative multiple case study was to explore strategies some small business owners in the retail industry used to reduce cyberattacks to remain profitable. The participants consisted of 5 small retail business owners in the central region of Alabama, who implemented successful strategies to reduce cyberattacks and maintain profitability. Based on the methodological triangulation of the data sources, and analyzing the data using Yin's 5-phase process, 3 themes emerged: business cybersecurity strategy, network security, and systems user access management. A key recommendation is to have a business cybersecurity strategy coupled with antivirus technology to negate small business cyberattacks. The findings may contribute to social change by providing small retail business owners strategies to mitigate the cybertheft of personally identifiable information. In turn, subsequently increasing consumer confidence and improving the financial stability of small retail businesses to create economic growth in local communities.

Maintaining Small Retail Business Profitability by Reducing Cyberattacks

by

Ira J. Phillips, Jr.

MA, American Military University, 2015

BS, Faulkner University, 1998

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

June 2020

Dedication

This research I devote to my wife, Pamela T. Phillips, and to both our sons, V'anthony I. Phillips, and Darien J. Phillips. To my mother, Ms. Susie M. Phillips, my aunt, Ms. Elizabeth McGowan, my sisters, Maple L. Phillips and Betty J. Dorman, and my brothers, Arthur B. Phillips, Donald M. Phillips, Debron L. Phillips, and O'Brian L. Phillips, I extend my devotion. Ultimately, I devote this study to anyone who, like me, was the first person to receive a doctorate in his or her family. Dedicate yourself to the real meaning and purpose of your life; make a positive difference in society.

Acknowledgments

Through his son, Jesus, I give glory to God. I thank God for placing me amongst his angels to help guide, inspire, and motivate me to make it through this journey. I am grateful for the mentorship and support of Dr. Krista K. Laursen for my prospectus acceptance. I am thankful to Dr. Alexandre Y. Lazo for his constant support and determination to drive me beyond my limits and ensure that I became an expert for my centered research. My first conversation with Dr. Lazo will always be in my mind. For such a pivotal moment in my life, I cannot thank Dr. Lazo enough. My study could not be completed without Dr. Julia East, Dr. Vania J. Bright, and Dr. Yvonne Doll being remembered. The support and upliftment from Dr. East came at the perfect moment during my first residency intensive retreat. Dr. Brights ' mentoring and editing skills sharing were invaluable during the completion of my study and I thank her for her unselfish support. Dr. Doll's encouragement during my second intensive retreat were invaluable. I am grateful for Dr. Janet M. Booker's and Dr. Ronald C. Jones' commitment to excellence and their unwavering support.

I appreciate Dr. Wileen Barosy, who took the time to call me every week and inspired me to continue to work harder on completing my doctoral study. I thank Erlinda P. Padua, who challenged me to complete my doctoral study in 2020. Each of the individuals listed above is responsible for the completion of this study. I am always thankful that you have shared me your time and expertise. To anyone desiring to pursue a doctorate, one's success is only restricted by the determination and sacrifices to be made.

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

Business owners collect and store a significant amount of personal data and most consumers do not approve of the secondary uses of their personal data (Kshetri, 2017). Most small and medium-sized enterprise (SME) owners lack the essential information technology resources and capabilities to implement preventive cyberattack measures (Harris & Patten, 2014). Cyber incidents in 2014 resulted in an average annual loss of approximately $400 billion (Arief, Bin Adzmi, & Gross, 2015). Disclosure of confidential personal data can potentially destroy reputations, constrain future actions, or undermine advantages gained through technological superiority (Schneider, 2018). Data breaches resulting in the theft or loss of private information can be expensive for any business (Piggin, 2016); however, SME owners may experience significant challenges and unrecoverable losses resulting from cyberattacks. Small business owners who gain knowledge of successful cybersecurity strategies may be able to successfully mitigate cyberattacks and maintain or increase profitability.

Background of the Problem

Data breaches are occurring with increasing frequency, causing businesses to incur substantial financial costs and to suffer losses of customer trust, revenue, and market share (Gwebu, Jing, & Li, 2018). Small retail business owners and their employees are among the over 2.3 billion people using computers with internet connectivity for business, learning, banking, and shopping (Central Intelligence Agency [CIA], 2015). Business owners need to be proactive in implementing new security strategies to protect their business and clients' personal data and maintain profitability.

Business owners and their clients are becoming increasingly vulnerable to cyber threats because of their increasing dependence on information technology (IT) for day-to-day business activities.

According to Giboney, Proudfoot, Goel, and Valacich (2016), the exploitation of computer systems and networks by computer hackers poses a continuous and unrelenting threat to small retail businesses. The exposure of over 153,003,441 personal records in 2015 from data breaches in the United States highlights the importance for business owners to establish strategies to reduce cyberattacks (Ashenmacher, 2016). Small retail business owners must understand that the aim of information security is to protect information from unauthorized access, use, disclosure, disruption, modification, and destruction (Mesquida & Mas, 2015). By establishing a cybersecurity strategy and managing information security risks, business leaders can potentially focus their efforts on protecting information assets and resources. My objective in this study was to explore the strategies that some small business owners in the retail industry use to reduce cyberattacks to remain profitable.

Problem Statement

As hackers develop sophisticated methods to penetrate security efforts, management team members across all types of businesses have become increasingly concerned about cybersecurity breaches (Beckett, 2015). Sixty percent of all targeted cyberattacks in 2014 struck small and midsize businesses, resulting in several hundred thousand dollars of revenue loss (Aguilar, 2015). The general business problem was that small business owners lack the resources to reduce or recover from cyberattacks and risk the loss of both revenue and business. The specific business problem was that some small business owners in the retail industry lack strategies to reduce cyberattacks to remain profitable.

Purpose Statement

The purpose of this qualitative multiple case study was to explore the strategies that some small business owners in the retail industry use to reduce cyberattacks to remain profitable. The targeted population was five small retail business owners in the central region of Alabama who implemented successful strategies to reduce cyberattacks and maintain profitability. The implications for social change include the potential for small retail business owners to mitigate cybertheft of personally identifiable information (PII), subsequently increasing consumer confidence and improving the financial stability of small retail businesses to create economic growth in local communities.

Nature of the Study

Qualitative research supports theory elaboration and theory generation instead of theory testing (Reinecke, Arnold, & Palazzo, 2016). I used a qualitative approach to explore strategies for maintaining the profitability of small businesses in the retail industry by reducing cyberattacks as this method is appropriate as a holistic framework for understanding the problem. Researchers using a quantitative method focus on applied and theoretical discoveries or findings that come from comprehensive research questions through field study in natural conditions (Park & Park, 2016). Researchers use the quantitative method to examine variables' relationships, differences, and causes of behavior through careful isolation, measurement, and evaluation of variables, focusing on predictability, process improvement, and control over time (Park & Park, 2016). I did not measure and evaluate variables' relationships or differences, so a quantitative method is not suitable for this research study. Researchers using the mixed method approach combine qualitative and quantitative methods and often include multiple theoretical perspectives in their studies (Hesse-Biber, 2015). A mixed method approach was not appropriate for this study because I did not include a quantitative component in my identification and exploration of successful strategies that some small business owners in the retail industry use to reduce cyberattacks to remain profitable.

Qualitative research designs include case study, ethnographic, and phenomenological styles (Arino, LeBaron, & Milliken, 2016). An exploratory study using a multiple case study design was suitable for this study. Researchers use a case study design to explore a real-life phenomenon in-depth and within an environmental context (Ridder, 2017). Researchers use an ethnographic design to observe participants' cultural behaviors over a significant length of time (Baskerville & Myers, 2015), which was not the objective of this study. According to Arino et al. (2016), researchers use a phenomenological design to explore the meanings of individuals' lived experiences to provide a first-person point of view. The purpose of this study was to obtain information on strategies for maintaining the profitability of small businesses in the retail industry by reducing cyberattacks, not to focus on the meanings of lived experiences of small business leaders. As such, a phenomenological design was not appropriate for this study.

Research Question

What strategies do some small business owners in the retail industry use to reduce cyberattacks to remain profitable?

Interview Questions

1. What business strategies do you use to reduce cyberattacks to remain profitable?
2. How did you develop successful strategies to reduce cyberattacks to remain profitable?
3. What strategies were not successful in reducing cyberattacks to remain profitable?
4. What, if any, key barriers existed in implementing strategies to reduce cyberattacks to remain profitable?
5. How did you address these key barriers to implementing strategies to reduce cyberattacks to remain profitable?
6. What additional information can you share regarding strategies for reducing cyberattacks that we have not already discussed?

Conceptual Framework

The conceptual framework for this study was general systems theory (GST). Von Bertalanffy (1972) developed GST as a framework for studying the interrelationships among modules that cause systems to be self-regulating and self-correcting. According to Drack and Schwarz (2010), the key tenets of GST are function, structure, and process. Researchers use GST to take a holistic view of organizational systems, including the exploration of experiences (Drack & Schwarz, 2010). Identifying potential gaps in employees' computer use experiences is an important measure for improving the protection of systems from cyberattacks. Researchers can view SMEs as systems consisting of various components, one of which is information security (Gomes, 2015). According to Atoum and Otoom (2016), cybersecurity for small business owners is a critical systems component. Von Bertalanffy's GST provided a lens for exploring how small business owners in the retail industry develop and implement strategies to mitigate cybertheft of PII and for supporting the overall functioning of other organizational systems within small retail businesses.

Operational Definitions

Cyberattack: A malicious attempt to gain access to a computer system or network to alter, disrupt, degrade, or destroy (Federal Emergency Management Agency [FEMA], 2018).

Cybersecurity: The collection of tools, policies, security concepts, security safeguards, risk management approaches, training, best practices, assurance, and technologies that can prevent or protect the cyber environment, the organization, and user assets (Von Solms & Van Niekerk, 2013).

Data breach: An incident that comprises unauthorized access to sensitive, protected, or confidential data, resulting in the compromise of the confidentiality, integrity, and availability of the data (Sen & Borle, 2015).

Social engineering: The exploitation of weaknesses by the manipulation of the victim into performing actions that benefit that attacker (Flores & Ekstedt, 2016).

Assumptions, Limitations, and Delimitations

Assumptions

According to Leedy and Ormrod (2015), assumptions are something the researcher accepts as true without tangible or intangible evidence. A total of four assumptions were relevant to this doctoral study. First, I assumed that semistructured interviews would result in enough data to answer the overarching research question. Second, I assumed that I would collect sufficient data to support triangulation. Third, I assumed there were no time delays during data collection. Fourth, I assumed that participants would provide truthful responses to the interview questions without personal bias.

Limitations

Yilmaz (2013) defined research limitations as constraints over which the researcher has no control and which may limit the transferability of the research findings to other situations. The first limitation was the availability of participants for personal interviews to support timely data collection. Participant access was critical for initiating data collection using the interview method; however, limits existed due to the participant's availability. The second limitation was that small business owners may inadvertently provide inadequate data due to a lack of knowledge about cybersecurity. In addition, the participants’ responses could include biased perspectives. The third limitation was that small business leaders may lack the appropriate knowledge to provide enough responses surrounding their cybersecurity practices. Interview questions and answers may not provide enough information to support the study.

Delimitations

Delimitations are specifics that limit the scope and variables of a research study (García, Skotnicka, & Zamora, 2015; Marshall & Rossman, 2016). First, I only included small business owners who had a license to operate a retail business in the southcentral region of Alabama. Second, I only included small business owners who employed between one and 100 employees. Third, I only included small businesses with annual gross revenues under $10 million. Fourth, business owners were delimited for participation with less than 5 years' experience. Fifth, researcher-imposed delimitations such as participants who were not interested in discussing their experiences. Finally, I only included small business owners who had successfully implemented cybersecurity strategies that reduced cyberattacks and helped maintain business profitability.

Significance of the Study

Business leaders are experiencing data infringements with increasing frequency, and these infringements present a risk to the financial stability and bottom line of their organizations (Manworren, Letwat, & Daily, 2016). Small business owners in the retail industry must protect their network infrastructure to maintain profitability in a potentially disruptive computing paradigm that is likely to change business processes and strategies (Vlad, 2017). Small business owners who gain knowledge of successful cybersecurity strategies may be able to successfully mitigate cyberattacks and maintain or increase profitability.

Contribution to Business Practice

Business owners who establish strategies to protect customers, consumers, and business partners' sensitive information may contribute to effective business practices. Business leaders must become adaptive, emergent, and self-aware to implement technology in a manner that supports and contributes to organizational survival (Sun, Wu, & Yang, 2018). Findings from this study may contribute to business practice by providing small business owners in the retail industry with strategies they can use to identify and address critical vulnerabilities within their network infrastructure and effectively combat cyberattacks that diminish profitability.

Implications for Social Change

Abundant computing power, the free flow of information on the Internet, and the ability to harness data are elements in a new socioeconomic paradigm for retailers and consumers (O'Neal, 2016). Social change is inevitable because of the threat of digital piracy leading to organizational innovation (Andersson Schwarz & Burkart, 2015). Business leaders face complicated cybersecurity standards and frameworks with no easy-to-understand toolkit to address their security needs (Mijnhardt, Baars, & Spruit, 2016). However, business leaders should recognize cybercrime threats and ensure the implementation of adequate protection measures (Eddolls, 2016). Small retail business owners may use findings from this study to develop and implement strategies to mitigate cybertheft of PII, enabling them to increase consumer confidence, improve the financial stability of their businesses, and contribute to economic growth in local communities.

Review of the Professional and Academic Literature

The purpose of this qualitative multiple case study was to explore the strategies that some small business owners in the retail industry used to reduce cyberattacks to remain profitable. Researchers use a literature review as a basis to identify, understand, and build on current materials applicable to the research question (Turner, Baker, & Kellner, 2018). According to Osanloo and Grant (2016), researchers use a literature review to help frame their study and develop a framework for the analysis of results.

I located peer-reviewed articles for this literature review from the following Walden Library databases: ABI/INFORM, Emerald Management Journals, ProQuest, EBSCOhost, Google Scholar, ScienceDirect, SAGE Premier, and Government databases. I searched these databases using key words such as *cybersecurity, cyberattacks, information technology, information systems, information security, small business owners, types of small business owners, GST, small business failure factors, small business success strategies, innovations, corporate social responsibility, leadership strategies*, and *leadership styles.* The literature review contains a total of 151 references, of which 94% (142) are peer-reviewed, and 90% (136) are published between 2016 and 2020.

General System Theory

The conceptual framework for this study was GST. Von Bertalanffy (1972) developed GST as a framework for studying the interrelationships among modules that cause systems to be self-regulating and self-correcting. According to Drack and Schwarz (2010), the key tenets of GST are function, structure, and process. Researchers use GST to take a holistic view of organizational systems, including the exploration of experiences (Drack & Schwarz, 2010). Identifying potential gaps in employees' computer use experiences is an important measure for improving the protection of systems from cyberattacks. SMEs are like systems consisting of different components, one of which is information security (Jordan, Bernardy, Stroh, Horeis, & Stich, 2017). According to Atoum and Otoom (2016), cybersecurity for small business owners is a critical systems component. Von Bertalanffy's GST provided a lens for exploring how small business owners in the retail industry develop and implement strategies to mitigate cybertheft of PII and for supporting the overall functioning of other organizational systems within small retail businesses.

Researchers have applied GST to various sets of systems. According to von Bertalanffy (1968), the center of GST is open systems and systems thinking. Open systems interact with their environment to either adapt or determine the best fit (Panda & Kapoor, 2017). Considering that most small businesses interact with their environment, components of the systems that do not function as designed can affect the overall functional equivalence of the system. A business is a network of interconnected parts whereby each part has a specific purpose and specific task (Buyya et al., 2018). The strategies that some small business owners in the retail industry use to reduce cyberattacks to remain profitable is one of the many parts that make up an organization or system.

Holism is a key tenet of GST. According to von Bertalanffy (1968), a holistic approach is ideal when designing any complex system. The central component of GST is the entire process, which is complete when all pieces work as intended (Rousseeau, Billingham, Wilby, & Blachfellner, 2016). The holistic approach is only one element of the overall organization system that some small business owners in the retail industry can use to reduce cyberattacks to remain profitable.

Another key tenet of general systems theory is entropy. Entropy is a measure of decay or disorder in a system (von Bertalanffy, 1968). Basically, a system will most likely have trouble or break down if not responsibly managed or controlled. Additionally, when a system experiences an increase in entropy, the system capabilities will decrease based on the belief that systems depend on a form of order and unity to exist (Van Assche, Verschraegen, Valentinov, & Gruezmacher, 2019). A business is composed of several subsystems at its core and each has a unique function or objective.

Over the years, researchers, scientists, and practitioners have used GST as one of their main theories. In 1973, von Bertalanffy first presented his idea of a GST (Wilson, 2012). The public received the first publication of a GST in 1946 (Thomas, 2015). One aim of GST is to explore the integration relations within natural and social sciences.

Von Bertalanffy (1968) hypothesized that GST is applicable to all sciences concerned with systems. Furthermore, according to von Bertalanffy (1972), the interconnection between the components of a system is more essential when compared to the components themselves. Interconnection is necessary because all separate components must act as a single system.

Since 1995, many contributions to von Bertalanffy’s original theoretical model of general systems by other researchers suggest that systems are both inputs and outputs working in coherence to satisfy objectives (Rousseau, 2015). According to Kast and Rosenzweig (1972), in the 19th and early 20th centuries, researchers' revisions to systems theory aim to accommodate social systems, communication, and other forms of holistic thinking. A holistic view within an organization is essential to ensure that all the components of the system are functioning properly and as designed.

A holistic view way of thinking forms the core of small business owners in the retail industry, as he or she must look at every element of the system/organization and determine what is functioning as designed and what elements need to be modified to reduce cyberattacks to remain profitable. Kast and Rosenzweig (1972) addressed several key concepts put forth over the years by many of the contributing authors (see Benton, GonzÃlez-Jurado, Beneit-Montesinos, & FernÃndez, 2013) such as feedback to improve or modify business practices or systems, a system's inputs and outputs working together to achieve the objectives of the system, and interrelated subsystems that are essential to business functions.

Most of the small businesses in the retail industry can potentially be an open system when viewing through the lens of GST. According to Von Bertalanffy (1972), organizations are either simple or complex systems. A complex system is one that includes subsystems and possible microsystems. Suter et al., (2013) suggested that GST addresses complex systems such as hospitals, schools, and organizations. Small businesses need separate divisions to work together to sustain the entire company.

An organization such as a small business within the retail industry is a complex system consisting of synergy, open systems, and subsystems. Open systems communicate with their environment (Panda & Kapoor, 2017), and either adapt or determine the best match for a specific task. Most small businesses are potentially open systems, which means they interact with their environment and this interaction helps determine nonfunctioning components of the system affecting the equifinality of the system. Growth has occurred in communities, organizations, and national and international institutions that enable them to become open information access networks that give way to the growth of various information accessible to society (Douglass, Garbaye, & Ho, 2019). Concerning the GST, the incorporation and coordination of information security management elements within an enterprise are necessary to minimize the effects on the business performance of information security threats.

Organizations usually contain several subsystems (Yi & Scholz, 2016). In applying the GST, small businesses are viewed as a purposeful system of interrelated subsystems working simultaneously with each other to achieve a common goal in an inconsistent environment (Wang, Shi, Nevo, Li, & Chen, 2015). A change or deviation in performance in one subsystem will impact the overall organization or system. No two employees' characteristics are the same and the social phenomena continue to evolve, creating new changes to modify the internal environment's structure and subsystems (Alter, 2018). Small retail business leaders need to remind workers of cyber surveillance using time stamps, security checks, flash drive tracking, and malware alerts through program adaptation and evolution (Conteh & Schmick, 2016). The possibilities of business owners inability to reduce cyberattacks continues to increase.

Synergy is an important concept for small business owners to understand. Units or subsystems of the organization flourish when they work in unity as oppose independently (Voinea, 2018). GST consists of inputs, outputs, and processes that foster a better understanding of how to improve a system's reliability and efficiency (Johnson, 2013). Researchers can use the GST to potentially gain a better understanding of the root cause of a system's problem that may lead to the development of a solution that ultimately makes the system more reliable.

Entropy is a vital concept to GST. According to von Bertalanffy (1968), the second principle in thermodynamics refers to entropy in a closed system as a quantity that must increase to a maximum until it comes to a stop at a state of equilibrium. Entropy is the measure of disorder or decay in a system (von Bertalanffy, 1968). According to Coole and Brooks (2014), the term entropy is challenging to envision and many times there are misunderstandings on how one central theme conveys how various components of a system connect to each other towards producing a coherent whole. A key objective for most businesses or organizations is the protection of its data by reducing cyberattacks to remain profitable.

One of the primary goals of many small retail businesses is information security. An essential element of a small business strategy is the protection of its information assets (Shedden, Ahmad, Smith, Tscherning, & Scheepers, 2016). At the center of information, security is the protection of the business's sensitive data from cyberattacks. One of the goals of small businesses or as a system is reducing cyberattacks to remain profitable and information security is a system within the business. A GST approach allows for an examination of relationships between two or more systems (Montgomery & Oladapo, 2014). Furthermore, GST enables the business to function as a whole system made up of several integrated parts all working to achieve the business objective to reduce cyberattacks to remain profitable.

An essential task for most small business leaders is to understand what constitutes a system and how each subcomponent interacts with each other. When small business leaders understand the systems theory, they will learn how to efficiently unify resources; subsequently, increase the chances of mitigating business risk to remain profitable (Prajogo, Toy, Bhattacharya, Oke, & Cheng, 2018). Business owners who pursue insight into the different elements of their business achieve business sustainability and effective structural systems (Cosenz & Noto, 2018). The constructs of the GST align with maintaining small retail business profitability by reducing cyberattacks by fostering an opportunity for business leaders to establish strategies to ensure the interdependence, interaction, and interconnection of all resources.

Alternative Theory

Systems theory encompasses contingency theory (von Bertalanffy, 1972). The contingency theory approach relates to problems that exist from within whole systems (von Bertalanffy, 1972). The interchangeable relationship of these theories relates to decision making and leadership (Meier, 2016). Strategic contingency theory keys in on a business leader’s effectiveness and strategies based on various factors that impact business operations (Shao, 2019). For this study, I explored the limitations of the contingency theory.

Each business is uniquely designed specifically for the organization’s operating environment. The primary focus of contingency theory is the relationship between the business’ design and performance (Micheli & Mura, 2017). Additionally, the performance results are the product of internal and external events influencing business operations (Fiedler, 1964). Many small retail companies create specific circumstances needing software customized to their distinctive characteristics to achieve optimum usability.

A dynamic use of contingency theory may help business leaders to take a systematic approach to matters pertaining to resources management and control. Business leaders who use contingency theory develop a predictive mechanism to ensure optimal control over the use of resources (Otley, 2016). Effective operations management practices may develop, measure, and ensure business performance. The construct of the contingency theory helps foster an environment whereby business leaders can identify essential parameters that may serve as a solid foundation to interconnect business systems together for efficient operation (Nofal & Yusof, 2016).

The ideas of the contingency theory are useful for business leaders to potentially develop an entrepreneurial mindset for business sustainability. The constructs of the theory provide an opportunity for business leaders to learn leadership and behavioral abilities that aid in effective business governance (Seibert, Sargent, Kraimer, & Kiazad, 2017). Business leaders can minimize business failures by gaining leadership abilities to ensure meaningful business practices; subsequently, maintaining profitability (Turner & Endres, 2017).

Applying the principles of contingency theory to this study may help small retail business owners maintain profitability by developing strategies to reduce cyberattacks. Most business leaders can plan and implement policies and strategies when employees are professionally managed, which may lead to high organizational performance and effective use of resources (Laureani & Antony, 2019). A contingency plan contributes to organizational performance (Turner & Endres, 2017).

The tailoring of business leaders' leadership style and management techniques to the specific business operating environment is important. The performance of business leaders depends on the environment in which the business operates (Fiedler, 1964). Contingency theory use by business leaders will most likely have many systems working cooperatively to achieve business success (Shao, Feng, & Hu, 2016). The ideas of contingency theory are to help business owners to adopt leadership, management, and motivational strategies to opposing business forces, which result in maintaining business profitability (Van Looy & Van den Bergh, 2018).

Cybersecurity Threats

Threats to cybersecurity continue to grow, evolve, and take new forms. The identification in 2015, which is 36% higher than 2014, of 430 million new unique pieces of malware highlights the growing threats (Symantec, 2017). Small retail business owners who use computers can describe their information security needs and strive to rely on systems that ensure confidentiality, integrity, and availability (Kakucha & Buya, 2018). Some small businesses are extremely vulnerable with the rising rate of technology adoption. Malware infections can potentially corrupt, steal, or exploit business and consumer data. Adopting a cybersecurity approach that offers a strong and adaptable layer of protection is essential for small retail business owners.

Besides malware, there is a ransomware risk. Ransomware is a type of malware that hackers use to take over users' computer systems, sometimes locking them out of their own computer system (Goldsborough, 2016). Small business owners typically have the same cybersecurity controls in place as end users, which makes them targets of ransomware. Hackers usually use ransomware as a tool with the intent to extort money from the persons or businesses they infect.

The internal threat. Internal factors too often give hackers access to data violations or cyberattacks. Interestingly, most hackers are mythically described as perceptual programmers in a dark room who are searching for software loopholes or technology lapses. Interpreting Taillat's (2019) attribution as a technique for establishing who committed the crime is fundamental, international, and domestic, to violence and disorders. Achieving the perpetrator requires alleviating psychological, organizational, and strategic uncertainty at three levels. These levels are strategic, operations, and tactical. To succeed in the organization's work, employees of a small retail business must possess diverse abilities, efficient management, leadership, and the capacity to consider constraints and challenges (Schoemaker, Heaton, & Teece, 2018).

Malicious insiders are a major threat to small retailers because they have the knowledge and have access to the business's resources. Such insiders are the ones who can easily launch attacks and cause more damage than others (Liang, Zhao, Wang, & Li, 2018). Therefore, small retail businesses are vulnerable to cyberattacks or data violations, as staff members, third party partners and even customers are not exempt from the data breach entry point (Onwujekwe, Thomas, & Osei-Bryson, 2019). Furthermore, the use of most technology is on a network with Internet connectivity. In addition to being easier to launch, Liang et al. (2018) wrote, internal attacks are potentially more destructive. Small retail business owners can expect financial losses, disruption to the business, loss of reputation and long-term impacts from a malicious insider attack.

There are many explanations for why normal workers are becoming internal threats. As Harrison, Dilla, and Mennecke (2019) pointed out and described as a lack of empathy or awareness, one definition is ethical problems. The dishonest insider has no dignity and does not feel any regret for the harm done to others. Problems may also include diminishing commitment or decreasing connection to the business. A potential result is the birth of employee fraud.

Employee fraud is consistent with moral consistency because of its malicious attack. Some insiders are affected by social isolation problems such as chronic problems with other people. Malicious insiders exhibiting the characteristics of an introvert may seem excessively reliant on a computer, suffer from stressful work-related events, such as sanctions or internal audits; however, it is the stressful experience of employees that tends to lead to a higher likelihood of a breach of security (Smith et al., 2018). The issues can emerge from, death of a family member, a breakdown of relationships or serious injury, suggesting that cynical insiders are emotionally unstable. The results can lead to negative responses within the workplace. The inability to meet certain requirements or personal goals is a cause for disgruntling workers, according to Voris, Song, Salem, Hershkop, and Stolfo (2018). Subsequently, the disgruntled worker develops a sense of disaster, loneliness and alienation that leads to frustration, bad behavior and stress.

Data threats. Data risks and vulnerabilities are ongoing and changing. The possible use of data that expose fault as vulnerabilities is a security threat (Kaukola, Ruohonen, Tuomisto, Hyrynsalmi, & Leppänen, 2017). Small retail business leaders' challenges consist of the sophistication and customization of data threats to circumvent established security controls or protection methods (Cabaj, Kotulski, Ksiezopolski, & Mazurczyk, 2018). The theft of data is a continuing threat to the company's personal information about its customers (Manworren et al., 2016). According to Christoffersen (2018), a threat is a risk to another person, place, or object. Continuing, disruptive and persistent threats to critical information for small retail business owners are significant problems (Kaukola et al., 2017).

The management between technology, growth, and innovation is a major challenge for business leaders. The goal is to continue recognizing the evolving risk and data security approaches in the changing landscape (Martin, Borah, & Palmatier, 2017). According to Hintze (2018), the data controllers are organizations, and other companies act as data processors are third parties. The understanding of this risk is based on the company's knowledge of the dynamics of data transfer, data rest and data protection to comply with compliance requirements (Calvard & Jeske, 2018; Hintze, 2018).

Additional risks to the business and personal data classes include cloud computing, IoT and 5 G technology. Such threats need complex safety strategies to improve the security of data (Au, Liang, Liu, Lu, & Ning, 2018; Kumar & Zeadally, 2017). Small retail business owners must understand the security challenges needed to implement the emerging scheme for data protection. Data protection is a present issue for business leaders as the world moves from 4 G to 5G. Chaudhary, Kumar, and Zeadally (2017) proposed the incorporation of software-defined networking (SDN), network service chaining (NSC) and mobile edge computing (MEC) to build a secure data sharing system with emerging cloud-based technologies. In cloud computing, specifically for mobile cloud-based devices, Au et al. (2018) promoted data protection, focusing on user-centric activities in identity authentication, data encryption, and data integrity management areas. Au et al. also proposed audio, video and bio-based data integrity verification based on biometric authentication, symmetric and asymmetric encryption and the use of audio and video data integrity tests for these types of data security strategies. Symmetric and asymmetric encryption is advantageous for cloud data security (Lozupone, 2018).

Credibility centers are a system focused on the credibility of a cloud-based service center and the data requester. Small business retail owners must consider their data to determine the best plan for the potential threat climate. Business owners eventually need to consider risks to their data and recognize data vulnerabilities to implement an appropriate approach to risk tolerance. Threats are advanced and tailor-made to bypass existing mechanisms of threat management (Cozzolino, Verona, & Rothaermel, 2018). Unmixed threats result in increased risks affecting the expense, credibility, efficiency, and competitive advantage of a business (NIST, 2018). The problem with recognizing threats is that threats include individuals, systems, and technology. Contributing to the accuracy to recognize threats are the security protocols that are introduced to combat threats by individuals or by process adjustments or technological innovations, improvements, and performance. Business leaders must continue to focus on detecting risks to their data to maintain an appropriate approach to risk tolerance.

Internal Controls

Small retail business owners may not understand that they are vulnerable to financial loss due to internal control deficiencies. In 2017, companies around the world incurred around 4 trillion dollars of fraud loss (Gepp, Linnenluecke, Terrence, & Smith, 2018). The call for action to correct serious problems began with the adoption by Congress of Sarbanes-Oxley law of 2002. Subsequently, researchers began to study systems of internal control within organizations. Processes of internal control play an important role in protecting business resources, maintaining coherence, reliability, and accountability. Small retail business owners can enhance efficiency by applying trustworthy internal controls (Grace, Vincent, & Evans, 2018). Internal control processes play a significant role in safeguarding business resources, ensuring coherence, consistency, and transparency.

The issue of internal control methods is important for small retailers. Several researchers believe that agency theory is a method for understanding effective internal performance control mechanisms (Bosse & Phillips, 2016). Businesses require internal control systems to provide their customers with reliable financial reports (Mutnuru, 2016). Internal control mechanisms ensure that the company goals are achieved by strategies, processes, and procedures (Mutnuru, 2016). Ensuring reliability, safety of information, and reporting efficiency are key for small retail business owners. Known issues of internal control include inadequate data security, increased errors, lack of proper monitoring and problems with upgrading current controls undergrowth. Most business owners use COSCO to calculate the internal control mechanisms that aid in the assessment of profit margins (Mutnuru, 2016). Internal controls will potentially improve company goal efficiency, minimize financial losses, and sustain profitability.

Controlling climate, risk assessment, information, and communication, monitoring and current control measures are the five components of the COSO system linked to internal controls (Rae, Sands, & Subramaniam, 2017). Even though the COSO system five components of internal controls provide an analysis and classification summary of the appropriate control measures, it may be useful for business owners to examine internal control processes to avoid and identify obstacles that could influence profit margins. The regulation system contains a voice known as the moral climate for top managers (Rae et al., 2017). The component of the control system sets the basis for the counterpart elements. The management system provides an entity with a framework that affects individual behavior (Shabri, Saad, & Bakar, 2016). According to Lai, Li, Lin, and Wu (2017), a strong control system reduces the chances of failure of the other four components. Business owners can analyze the voice of executives at the highest level to ensure that business goals are met. The control system acknowledges that top managers reinforce ethical values that drive actions and decisions to achieve business goals. Lack of control components will adversely affect profit margins for companies (Lai et al., 2017).

A risk assessment is the second component of internal controls outlined in the COSO system. Risk assessment includes the ability of business owners to identify and quantify risks to reduce risk potential (Rae et al., 2017). Lyon and Popov (2017) suggested in their research study that risk assessment is a method of assessing and recognizing risks that can impede business goals from being achieved. Business owners may gain an understanding of strategies of risk assessment that can potentially increase profit margins. Small retail business owners can perform a routine risk assessment to identify potential risk areas and risk management approaches (Shabri et al., 2016).

Businesses use information and communication systems to easily register, store, share and communicate information. The quality of information and interaction influences the management's ability to manage and control business operations (Rae et al., 2017). Clear information and communication enable management to determine the effectiveness and risk assessment of internal control processes. Frazer (2016) has, for instance, revealed that information systems produce financial reports on the results of a company and the activities necessary for decision making. The system of effective communication allows parties such as investors, administrators, and clients to acquire and pass on pertinent information (Shabri et al., 2016).

Monitoring is another aspect that ensures the reliability over time of the internal control systems. Monitoring is an internal control process applicable to reduced agency costs (Yoo, Park, Back, & Hong, 2017). The monitoring learning includes the ability of management to assess if the internal control mechanisms work properly and therefore must adjust in changing environments (Frazer, 2016). Business owners may find tracking useful to determine the quality of management and ongoing plans to improve internal control processes.

The control activities may include policies and procedures chosen and developed for addressing risk, reporting reliable financial information, and ensuring business objectives are fulfilled (Rubino, Vitolla, & Garzoni, 2017). At all stages of a business operation, control activities can occur. According to Rae et al. (2017), a monitoring system is critical to maintaining the reliability of the control systems. Business owners may consider reviewing current control activities to assess whether the activity is still acceptable.

Small retail business owners create internal control processes for ensuring the efficiency of the business. Shabri, Saad, and Bakar (2016) studied the effects on company productivity of internal control methods. To evaluate the impact of internal control systems, the researchers applied the five internal control elements of the COSO model. The operating profit margins are an assessment indicator to allow internal control systems to assess their performance. Shabri et al. reported that COSO internal control systems find financial losses and measurement quality to be adequate to avoid. Organizations may also incur financial losses because of an insufficiency of cost control. Strong internal control systems will boost cost control, increase and sustainability (Shabri et al. 2016). COSO's internal control systems architecture is a critical factor in helping companies achieve their goals while also tracking performance.

Business owners help to manage the financial resources of the business to achieve the desired result. Once problems arise, business owners may find that internal control mechanisms require improvement to prevent restructuring, reductions in profit margins and negative financial performance (Omar & Rahman, 2019). Researchers examined the reasons for the existence of internal control measures in companies. According to Frazer (2016), the reasons for exiting internal control mechanisms are caused by major corporate scandals and the loss of key employees. Internal control systems are components of the efficiency and function of the organization's internal control system. Internal control systems allow business owners to verify that financial information is reliable and accurate (Frazer, 2016). Raiborn, Butler, Martin, and Pizzini (2017) supported Frazer's (2016) findings by evaluating the benefits of applying internal control processes. Raiborn et al. (2017) outline a method to help businesses minimize nonvaluable activities, increase profitability and a better understanding of the control system and structure in enforcing internal controls. Internal control systems help to foster an environment for business owners to check that financial information is reliable and accurate (Rendon & Rendon, 2016).

Companies tend to invest in a system of internal control that helps to achieve better profit margins. Small retail business owners must consider concentrating more on establishing internal controls and less on enhancing and improving the mechanisms of control (Afriyie, Kong, Danso, Ibn Musah, & Akomeah, 2019). The reliability of internal controls guarantees transparency. The findings from Afriyie et al. (2019) indicated that market productivity relates to the performance of internal control processes.

The falsification of financial reports by corporations has intensified the need to improve internal control mechanisms. Frazer (2016) studied the impact of improving internal controls to prevent unethical actions by managers. The lack of internal control mechanisms can lead to financial difficulties for small retail businesses. In Frazer (2016) research, there is less fraudulent behavior for businesses with better internal controls. If the owners of companies fail to implement internal controls, the risk of fraud and loss rises for the company (Zager, Malis, & Novak, 2016). Internal control systems are mainly designed to protect business assets while at the same time meeting their development and profitability objectives (Mutnuru 2016). The quality of monitoring allows business owners to circumvent ethical behavior. Other researchers identify shortcomings in internal control processes that impact business profitability, performance, and sustainability (Harp & Barnes, 2018). Appropriate internal control mechanisms will most likely increase the operational capability of the business.

To manage and regulate the decision of managers, internal controls are necessary. Internal controls are measures that restrict actors to take decisions of themselves, but which follow the interests of the principal (Kultys, 2016). Internal control mechanisms over agents may include properly structured workers, standardized salaries, duties delegations, main bond agents and task break-ups. The purpose of the Internal Control System is to ensure that the policies and procedures developed by the Controller are effective and fulfill the mission of the organization (Mutnuru, 2016). Through introducing active internal controls, organizations will mitigate the risk of failure (Mutnuru, 2016).

Business investments will drive growth and profitability. Lee, Cho, and Choi (2016) studied the shortcomings in investment performance internal controls. Industries tend to spend surplus funds outside operating activities on capital investment. A company's productivity depends on how investments are made (Lee et al., 2016). Lee et al. showed that companies with internal control deficiencies lack strategies to monitor the actions of managers that may be different from making optimum investment decisions. The use of internal control systems allows business owners to spend excess cash assets to increase profitability (Arouri & Pijourlet, 2017). Internal control systems enable business owners to effectively protect and use cash to increase their business value. The lack of internal controls means businesses can restrict their ability to increase profit margins. Bauer (2016) explained that, because of weaknesses in internal controls, managers can make poor investment decisions that impact costs. Some purposes for internal control systems are to increase company performance, optimizing financial reports and compliance with regulations.

Principles of internal controls. There is no real system to ensure productivity. Clear internal control standards can help an organization avoid damages and failures arising from mistakes and fraud. Internal control systems often provide specific guidelines on internal control principles, leaving the implementing organizations with specifics (Gal, Länsiluoto, Jokipii, & Eklund, 2016). Rija and Rubino (2018) clarified that internal controls are an important tool in the pursuit of business goals and, at the same time, avoid wasting money, protect business assets, produce information on accounting and maintain efficiently, comply with plans, policy and business procedures and, in particular, ensure compliance with legislation and regulations.

Business owners can create sound ideas leading to a controlled environment. The purpose is to help companies to enhance their processes and manage business functions. To implement effective systems, business owners should understand the relevance of internal control processes for building quality. The U.S. Congress introduced the 2002 SOX to curtail the unethical conduct of business owners. Internal controls are techniques business owners can use to prevent theft, fraud, and misappropriation of business assets (Bentley-Goode, Newton, & Thompson, 2017). Also, internal control mechanisms can be a buffer so that reports of accounting data are true, reliable, and correct (Bentley-Goode et al., 2017). Implementation of successful internal control mechanisms will strengthen customers' trust and confidence in business financial documents. Stakeholders rely on business financial reports when making an investment decision (Gao & Jia, 2016). The owners of small retail businesses must consider introducing management processes to minimize interventions that have a negative impact on profit margins.

Corporate governance. Increasing fraud scandals enhances the need for companies to review their corporate governance policies. Corporate governance is an important element in the internal control systems of organizations (Zuckweiler, Rosacker & Hayes, 2016). Researchers proposed that the philosophy of the agency would lay down the corporate governance study structure (Shi, Connelly, & Hoskisson, 2017). The organization theory helps in the recognition of social changes in society and the need for corporate governance (Kultys, 2016). Corporate governance is a specific set of policies that encourage accountability, honesty, and fairness by presenting important decision-making data (Shi et al., 2017). Corporate governance principles agree with the recruitment of appropriate people with decision-making rights and responsibilities. Corporate governance frameworks describe organizational control and management interventions (Shi et al., 2017). Some small retail businesses may not be able to devise management strategies for sustainable economic growth and avoid fraudulent behavior. The lack of transparency in the retail industry contributes to more needless business controversies and financial collapse.

Studies by researchers on how corporate governance impacts organizational quality and shareholders are relevant and of importance. Central corporate governance policies ensure the protection of stakeholder interest in the company (Silva Martins & Ventura Júnior, 2020). Ahmed and Hamdan (2015) explained how corporate governance policies improve ties between the corporate owner and the stakeholder. Corporate management practices, as set out in Prokhorova and Zakharova (2016) also improve client reputation, transparency and reduce risk. Business owners can increase the confidence of investors in financial reports through active corporate governance practices. Blockchains are a new application to old financial recordkeeping problems in cryptography and information technology and could result in significant management changes (Yermack, 2017).

Trust between investors and lenders began to decline in the early 2000 corporate scandals. The public disgrace's consequences prompt investors to press business leaders to take action to protect their investment. The implementation of corporate governance policies is useful to maintain and attract investors, to measure their quality and to inspire management decisions (Muller, 2009). Ruggiero and Cupertino (2018) explained that investors are more likely to provide companies that follow corporate policy with financial resources. Corporate governance legislation is a tool to determine productivity for business owners. Education can potentially provide business owners with the instruments required to assess and track company financial health.

Corporate management strategies set the tone for corporate operation and direction. Agyei-Mensah (2016) notes that corporate governance illustrates the necessary procedures to supervise the corporate structure. The foundation of governance is the collaboration and control process in the interest of investors (Agyei-Mensah 2016). Promoting corporate governance among corporate owners and shareholders improves their relationship (Agyei-Mensah, 2016). Small retail business owners choose to handle the finances of their businesses as a direct result of their personal goals for a company (Wong, Holmes, & Schaper, 2018). Business owners can potentially build market confidence and attract positive investment by minimizing fraudulent activities.

New technologies allow fraudsters to develop their methods of illegally accessing sensitive data and documents within a business. Significant losses arising from fraud and cybercrime may result in the company losing part of its profits and may result in a decrease in investment attractiveness and potentially damaging the brand (Radchenko, Kolodeznaia, & Karpovich, 2019). The standard of corporate management procedures directs the use of assets and control measures to reduce fraud and income losses for the designated agent (Silva Martins & Ventura Júnior, 2020). In addition, effective corporate governance practices help to improve the ethical conduct, transparency, and accountability of financial documents submitted to investors (Silva Martins & Ventura

Júnior, 2020). The corporate governance elements affect the internal control mechanisms defined in financial reporting.

The main goal of an organization is to maximize revenue and control costs. Corporate governance structures are therefore adding an additional layer by securing investors and economic stability. Although the intention is to increase profitability, it may be important to implement and enforce actions to protect economic sustainability. Companies with profit loss were trying to reduce their unfavorable performance by strengthened corporate governance policies (Liang, Kuo, Chan, & Chen, 2018). The moderating impact of corporate governance shows that better corporate governance could influence its development strategy, leading to better corporate results (Brahmana, Brahmana, & Fei Ho, 2018). Good strategies must be enforced to deter financial losses and fraud.

Internal controls and technology. Innovation is a growing demand and may have an impact on performance for small retail companies. Internal control mechanisms to respond to technology, therefore, need to be introduced. A corporate culture can influence internal technology system control processes. Sherif, Pitre, and Kamara (2016) conducted a study to explore technology control mechanisms for companies for mitigating nonethical behavior. Managers ' tones also form the principles of active technical controls (Sherif et al., 2016). To integrate internal control processes into software systems, information integrity is maintained, mistakes are minimized, an unethical activity can be detected and avoided that can influence productivity (Sherif et al., 2016). Technology is often useful to improve internal control processes. The types of technology controls include password protection, data access authority, authorization, and audit trails (Sherif et al., 2016). Businesses that perform internal control activities tend to detect fraudulent behavior. To discourage unethical conduct, technical regulation is an important process for internal control.

Cybersecurity Strategies

Employees must enforce formalized processes, procedures, and organizational controls of their business owners consisting of information technology security policies to identify the correct use of information and technical resources (D'Arcy & Lowry, 2019). James (2018) reported that 95% of business leaders identified cybersecurity as a highly, important field, but 45% did not have a structured approach. Results from Schneider’s (2018) study indicated that, 80% of small businesses do not have a cybersecurity strategy. Small retail business leaders should rethink cybersecurity strategies for the defense of shareholder benefits and prevent regulatory fines (James, 2018). Business leaders must maintain an integrated approach to cybersecurity, suited to their business and risk profile, concentrating not only on the technical aspects of their advocacy but also on the people and organizational elements in order to counter the emerging cyber-threat facing organizations (McGarry, 2016).

Some scholars identified potential cybersecurity approaches in literature. Business leaders can match organizational enterprise processes with security practices by integrating risk management of information security in an organization (Barafort, Mesquida, & Mas, 2017). Small retail business owners need to consider the strategic impacts of a cyberattack to resolve an assault on their information systems (Copeland, 2017). To ensure the World-wide Web (WWW) is a transparent and inclusive forum, business owners will need to engage in a globally different set of views, in new and creative ways, rather than in the traditional lines of the stakeholder groups (Sepulveda, 2017). In contrast, a cooperative, practical relationship focused on the shared information between the private and government sectors needs a solution to prevent and mitigate cyberattacks (Bell, 2017).

Small retail business owners must resolve possible vulnerabilities of products, strengthen network communication efficiency, and protect customer confidentiality. Selznick and Lamacchia (2018) argued that small businesses are easy prey to hackers because of their limited resources and technical skills. In tandem with Selznick and Lamacchia (2018), Watad, Washah, and Perez (2018) indicated that small business leaders must recognize that IT protection is a business requirement and a business expense. Inverse, Mrabet, Kaabouch, Ghazi and Ghazi (2018) suggested a three-tier cybersecurity strategy that consists of pre-attack, attack, and post-attack. Some business owners recognize the importance of leadership in the implementation of cybersecurity policy. A strong internal boss, often a chief information security office officer, who has worked with legal experts to direct the company before, during and after a crisis, is key in security governance procedures (Karanja, 2017). Human resources managers can help to create, interact, and cascade rules and procedures to keep the business secure by collaborating with the cybersecurity team, the full corporate-level management suite, and the board (Karanja, 2017). Failure to comply with information security policies is a potential problem for small retail leaders.

Leadership has driven policymakers to get interested parties engaged within their jurisdictions and internationally in the identification of good faith approaches, ranging from connecting all people in the world to ensuring that communication is secure and useful (Sepulveda, 2017). In comparison, Safa, Maple, Watson and Von Solms (2018) indicated that management should be aware of the environmental factors that motivate workers to commit misconduct in information security. The influence of management can be defined as views applied according to an organization's procedures or policies. Management can be one of the main impediments in preventing enhancing cyber resilience; thus, a lack of management support can be a devastating factor (George, 2016). The world is changing; the philosophy of management must also change. Society should become aware of new and evolving trends. Furthermore, small retail business leaders may consider looking at areas where culture has not yet become intuitive, such as cyberwar, as managers typically concentrate on budgets, efficiency, and timetables with little or no attention to cyberinfrastructure. A proactive management approach is potentially conducive to positive cash flow, competitive advantages, profitability, and business growth. As a promoter of business success, management requires commitment to protect the most valuable assets of the company (Fink, Yogev, & Even, 2017).

In addition to deciding the voice of the organization during a crisis, management is often the first voice of the organization and knows that rapid response is needed. The role of the Board and how it might be appropriate for the Board to be a leader in discussion, in crisis planning, is a key factor. While the board of directors expects members to defend them from cyberattacks, the directors are usually unprepared for this mission, and 58% of the board members describe cyber-related threats as being their most daunting risk (Rothrock, Kaplan, & van der Oord, 2018). The company could be at higher risk without good contact between the board of directors and the management (Greene, Gupta, L'Helias, & McCracken, 2017). The Board's role in cyber risk control cannot overestimate the importance of a comprehensive dialog with management.

Response plans. Incident response plans (IRPs) should be a key priority, yet many organizations are still developing action protocols. Collier (2016) has described the different phases or techniques required for protecting staff, evaluating accidents, safeguarding, and retrieving information, and any event-distressing situations. Brown (2016) found that 72% of companies have a plan in place to reduce potential costs related to crisis management, harm to reputation and loss of business interruption. An effective response plan is imperative to a business that decreases a cyberattack's fiscal impact. When a business produces an information infringement action plan, the risks, costs, and destruction of the event can be reduced. Six steps were identified by Collier (2016) as key to an effective IRP including planning, detection, containment, eradication, regeneration, and learning.

Security analytics (SA) is a new threat detection tool. The launch of SA allowed professionals to use work-intensive development software; however, simplification was accomplished through new programs including Prelert, Structured Query Language (SQL) and Lightcyber. SQL can include a broad range of criteria to determine which rows the user wants to find (Lino, Rocha, Macedo, & Sizo, 2019). When a business uses new technologies continuously, systems penetration techniques are constantly changing;

subsequently, becoming complex. The practices in cybersecurity should also evolve regularly and be no longer restricted to IT administrators. Cybersecurity practices require frequent adjustments and cannot be limited to IT managers. Cybersecurity includes employee participation.

Management has a responsibility to work with stakeholders to build an interface that describes the most and least cyberthreat vulnerabilities of the business and the risk management measures in place. Greene et al. (2017) noted that boards of directors need valuable measurements and analytical tests to determine if business managers handle cyber risk at an acceptable level. Management boards can also inquire about the use of risk management devices in a business. Through carrying out cyberattack scenarios and other training drills, business owners can recognize vulnerabilities and preparedness gaps and strengthen management teams ' ability to make decisions under stressful circumstances. Successful business owners directly involve management in these activities (Greene et al., 2017).

As the WWW expands, the potential for threats also arises. Researchers use IoT in different environments depending on their skills or experience (Qu, Thürer, Wang, Fu, Li, & Huang, 2017). The security of the Internet of Things (IoT) goes beyond domestic control. IoT surpasses refrigerators, which can order fresh milk and creates a larger void in the need for skilled workers and those who can fill the gap. IOT exceeds refrigerators, which can order fresh milk and generates an increased need for skilled workers and those capable of filling the gap. The implementation of IoT fosters an environment that can significantly minimize the information gap. The use of IoT enables a timely, reliable, and high-quality knowledge base to be established. IoT enables the interaction between networks and items that we use daily; the use of IoT often contributes to society's technology dependency so much that areas of interest include shopping online, entertainment, and healthcare. The new technology provides many useful advantages and rewards, as well as many obstacles such as personal device hacking (Zubiaga, Procter & Maple, 2018). IoT is projected to be fully functional in 2020 with approximately 26 billion people having Internet access; subsequently, only one entry into one device will allow a cybercriminal the chance to access all computers on a personal or business server (Hall, 2016). There is no clear indication of initiatives successfully resolving the complexities of IoT; unfortunately, allowing for continued cyberattacks.

Artificial intelligence (AI) is also new to the world of technology. Some researchers refer to AI as machine intelligence, as it is an algorithm for machine learning. The knowledge of a computer could have a positive global impact; however, can cause severe social and ethical problems (Grosz & Stone, 2018). Artificial intelligence systems can interact efficiently with people and through links with large data sets, robots, computers, and language systems. Artificial intelligence is a primary target for hacking. A vigorous awareness-raising drive by small retail business owners has contributed to the surge of individuals joining cybersecurity professions. Research by Mithas, Kude, and Whitaker (2018) indicated that there is a shortage of six million cybersecurity professionals. The lack of these resources represents a global capacity shortfall in human capital. With no adequate foreign cybersecurity professionals, business owners face a challenge to keep up to date with new technology and infrastructure to handle emerging cyber threats. Artificial intelligence can typically reduce staff. However, software developers in India account for 70% of global IT offshore work and 40% of IT-friendly business processes (Mithas et al., 2018). A greater chance exists for the programming profession to decrease because of AI (Mithas et al., 2018). Small retail business owners and large company owners alike must build specific awareness campaigns to ensure that everyone knows how to safeguard oneself when using technologies such as office systems, smartphones, or social media outlets.

Data loss prevention. The loss of data in organizations happens both internally and externally. The staff of Data Loss Prevention (DLP) must handle all insiders and outsiders who target their data to avoid the loss of data. DLP is data protection in transit through system processes to prevent data loss (Graves, 2017). Information loss is avoided through the development and review of cyber threats and risks infrastructure (Cheng, Liu, & Yao, 2017). The difficulty of DLP with specifications and controls to prevent future cyberattacks is a potential concern for most small retail businesses. Through monitoring cyber threats and network risks, business owners may prevent data loss (Shetty et al., 2018). Vitel and Bliddal (2015) used cybersecurity in France as proof of the implementation of the concepts and controls of the DLP. French cybersecurity experts were able to prevent data loss, including an awareness of threats across counter-attack techniques through on-line settings, protection, and enhanced cyber-crime information. Plachkinova and Maurer (2018) used the Target data infraction to demonstrate how cybersecurity and customer loyalty is enhanced by data loss response policies. One aspect of DLP is efficient support for the right leadership. Business owners must consider best practices in DLP, including (a) proper device management, (b) data management, (c) password and authentication use and (d) credit card tracking, and cyberattack prevention.

DLP is an awareness-raising mechanism for the physical protection of data, data loss prevention and data loss response. The DLP approaches include the categorization of data, user identification, and monitoring and limiting access to data (Graves, 2017). In this situation, IS / IT practitioners depend on intrusion detection systems (IDS) for cyberattack detection (Hajisalem & Babaie, 2018). Understanding cybercrimes and how techniques are being employed by hackers is important. IDS is an alert system allowing the network administrator to stop intruders' corporate network access and data loss (Hajisalem & Babaie, 2018). A data recovery plan is necessary when companies fail to implement adequate DLP measures.

As a means of remaining open, small retail business owners must establish a strategy for solving cybersecurity theft issues. Creation of an internal control and anti-fraud system for small companies with fraud risk assessment, control activities and information documentation may help reduce or end cybersecurity concerns (Dawson, Dawson, Eltayeb, & Omar, 2016). The basis for a business anti-fraud program is focused on management's routine research and understanding of business processes (Peltier-Rivest, 2018). Managers whose job is to review the company's internal controls will assess whether workers comply with established business processes and examine their work to determine whether the company has potential fraud (Peltier-Rivest, 2018). The disclosure of deception and cyber security threats can therefore potentially increase prevention if the owners of a company properly execute internal controls.

The implementation of internal control policies is important for alleviating the threat of theft and fraud. A comprehensive anti-fraud and cybersecurity system will greatly reduce internal threats of fraud and losses (Dawson, et al., 2016). Paulsen's (2016) research reinforces Dawson's et. al. (2016) research in that small business leaders can be agile and adaptive to change through cybersecurity. Through this adaptation, small business owners can handle cyberattacks and fraud-related issues more effectively than large organizations (Paulsen, 2016). The primary objective is for small retail business leaders to have a well-defined strategy to address cybersecurity and prevent data loss.

Cost of Cybersecurity Breaches

Networks are susceptible to hackers and cybercriminals interrupting. A cyberattack is a hacker's attempt to damage or disable a computer network or Internet-linked device (Škrjanc, Ozawa, Ban, & Dovzan, 2018). An assault on the cyberinfrastructure is to mismanage machine, technology-dependent companies, and network systems (Zhang, Wang, Liu, Ding, & Alsaadi, 2018). Cybercrime attacks, for example, challenge existing cybersecurity standards for electrical utilities to protect critical assets, interconnected dependents, and public safety from cyber threats (Smith, Corzine, Racey, Dunne, Hassett, & Weiss, 2016). Cybercrime is the insidious concern for small retail business owners; subsequently, owners ' efforts to promote universal access to IT fail, as some business leaders lack cybercrime or IT expertise in the interests of preventing related problems (Jayakar, 2018). Cybercrimes are problems that will unlimitedly harm the privacy, finances, and reputation of companies if ignored. To alter computer code and data, cybercriminals use malicious code to cause interference that can damage information and lead to cybercrimes such as data and identity theft (Burnap, France, Turner, & Jones, 2018). Cyberattacks continue to plague companies, forcing business owners to develop or adopt well-developed security plans to deter breaches of security.

Cybercrimes will cost businesses trillions of dollars. Sony sustained both physical and fiscal damage from a massive cyberattack. Sony’s $20 million in revenue loss and its loss of $32 billion due to a lack of customer data management is surreal (Hou, Gao, & Nicholson 2018). After this incident, Sony's cybersecurity management team began a preventive process that is known as a moving target defense to counter cyberattacks (Ghourab, Azab, & Mansour, 2019). Goal protection is a kind of security technology that deliberately alters IT infrastructure to prevent specific cyberattacks (Park, Woo, Moon, & Choi, 2018). Prevention of cyberattacks, particularly repeated attacks, is important for all companies. Business owners are trying to keep their data secure. Unfortunately, hackers are finding ways of intercepting private personal data that include spending millions of dollars on behalf of clients and creating client personal accounts vulnerabilities.

The damage that cyberattacks cause is increasing business owners’ cybersecurity defense expenses. Professionals in cybersecurity require an innovative protection strategy to minimize cyberattacks. The Web is one of the main drivers of national and international innovation, growth, and competitive advantages. In critical infrastructure management, public security, and consumer privacy (Ding, Han, Xiang, Ge, & Zhang, 2018) cyberattacks are significant concerns. Connection to corporate funding is one of the best ways of improving small business owners’ resilience. Small businesses are an essential component of the national economy, but some business owners do not regard themselves as cyberattack targets, creating a major gap in business security (Small Business Association, 2017). The increasing costs of cybersecurity make companies unsustainable and these costs are expected to increase rapidly.

In this technological era, network-based systems face new everyday cyberattacks. Traditional cybersecurity solutions are based on old data bases of threats and must be modified every day to counter cyber-threats in the new generation and protect underlying network-based systems (Usman, Jan, He, & Chen, 2019). In addition to updating threat information databases, it is critical that data generated by sensitive real-time applications are responsibly managed and processed. Organizations need to invest in cybersecurity training and awareness programs to motivate staff to participate actively in the development of their security policies to help people recognize and improve their computer security conduct (He & Zhang, 2019). Awareness of good cyber security requirements can make people understand the importance in protecting the cyberinfrastructure and lead to a change in behavior (Humaidi, & Balakrishnan, 2018). Training programs and educational materials will connect cyber awareness with the personal lives, families, and homes of staff to potentially make them more involved and possibly inspire the staff to improve their cybersecurity behavior.

Transition

In Section 1, I provided the foundation of the study that includes the background of the problem, problem statement, and purpose statement. I also presented the nature of the study, research question, interview questions, conceptual framework, operational definitions, assumptions, limitations, and delimitations. I provided the significance of the study that includes a contribution to business practice and the implications for social change. I concluded Section 1 with a review of the academic and professional literature relevant to maintaining small retail business profitability by reducing cyberattacks.

In Section 2, I will provide a discussion of the role of the researcher, participants, research method and design, population and sampling, ethical research, data collection instruments and techniques, data organization techniques, data analysis, and reliability and validity of the study. In Section 3, I will present study findings and will discuss the application of findings to professional practice, implications for social change, recommendations for action, and recommendations for further research. I will end Section 3 with my reflections.

Section 2: The Project

The focus of this qualitative multiple case study was to explore small business owners' strategies to reduce cyberattacks to remain profitable. I collected data for this study from leaders of small retail businesses using semistructured interviews and a review of company documents. In Section 2, I restated the purpose of the study and discussed the role of the researcher, research participants, research method and design, population and sampling, ethical research, data collection instruments, techniques, organization, and analysis. I concluded with a section about dependability, credibility, and confirmability.

Purpose Statement

The purpose of this qualitative multiple case study was to explore the strategies that some small business owners in the retail industry use to reduce cyberattacks to remain profitable. The targeted population was five small retail business owners in the central region of Alabama who implemented successful strategies to reduce cyberattacks and maintain profitability. The implications for social change include the potential for small retail business owners to mitigate cybertheft of PII, subsequently increasing consumer confidence and improving the financial stability of small retail businesses to create economic growth in local communities.

Role of the Researcher

I served as the primary instrument for this qualitative multiple case study for the collection and analysis of data. According to Chan, Fung, and Chien (2013), the researcher is the primary instrument for data collection and analysis in qualitative research. Additional responsibilities of a qualitative researcher include reviewing available information, identifying, and engaging with participants, collecting, and organizing data, conducting data analyzing and interpretation, and storing and securing data (Yin, 2012).

As the researcher, I was the interviewer and primary data collection instrument for this study. I am a military security cooperation director and a subject matter expert in information security risks and management systems. I have over 8 years of experience in the information sharing and cybersecurity environment, primarily through policy writing, process implementation, and process enhancements. My motivation to carry out this research stems from my familiarity with the research topic and the desire to enhance my knowledge from reviewing relevant academic and professional literature that supported the study. Before the start of this study, I had no relationship with the study participants. Furthermore, I had no business relationships with organizations or study participants.

A qualitative researcher is well versed in methods to reduce risks for participants (Velardo & Elliott, 2018). I avoided asking leading questions during the interview session to mitigate bias. Onwuegbuzie and Hwang (2014) proposed that researchers should refrain from asking leading questions to prevent bias. I ensured that the data collection remain unbiased by selecting study participants that I had no personal or business relationship. Throughout the interviews, I encouraged the study participants to speak openly, and completely, to capture their point of view accurately. According to Baškarada (2014), researchers must remain neutral to avoid influencing participants' answers in any way and must also refrain from gestures or comments that may alter participants’ responses. I avoided unnecessary body movement and potential persuasive verbiage that would potentially suggest to the study participant to alter a response.

As the researcher, I adhered to research ethics and *The Belmont Report* research protocol. A thorough understanding of *The Belmont Report* aids a researcher by ensuring that respect for participants is above reproach, maximizing the benefits of the study design while minimizing risks, and selecting research participants impartially (Fiske & Hauser, 2014). *The Belmont Report* is a synopsis of ethical principles and guidelines for research involving human subjects (Pearce, Ensafi, Li, Feamster, & Paxson, 2018). According to Resnik, Miller, Kwok, Engel, and Sandler (2015), the Protecting Human Research Participants (PHRP) training offered by the National Institute of Health (NIH) Office assists researchers in the informed consent process, in the protection of participants, and in dealing with ethical challenges in research. I used *The Belmont Report* to foster an environment that was respectful for my study participants and minimized potential risks that could have potentially related to the research process. In addition, I handled every participant ethically by fostering a comfortable environment and having a clear understanding of the process for their safety and well-being.

My objective was to conduct interviews that allowed the research participants to express their knowledge and insight on data security within their organization. I developed and used an interview protocol (see Appendix A) to guide my efforts to collect reliable data and ensured consistency within each interview process. According to Foley and O’Connor (2013), researchers develop and use an interview protocol as a guide during interviews to support the collection of reliable data and to ensure consistency of the interview with each participant. An interview protocol contains the interview questions and step-by-step guidance that a researcher can use consistently for several interviews (Penuel, Farrell, Allen, Toyama, & Coburn, 2018).

Participants

I identified potential participants who had the prerequisite knowledge to answer the central research question for this study. Yin (2017) noted that there must be experience in qualitative research with the phenomenon. Moustakas (1994) suggested that the researcher should find participants with knowledge and expertise to answer the research question in a qualitative study. Participants need to be able to provide facets and insights on a qualitative research phenomenon (Northrup & Shumway, 2014). Using a purposeful approach, I selected five small retail business owners that met the eligibility criteria for participation. The eligibility criteria for this study was a business owner of a small retail business in the central region of Alabama who implemented a successful strategy to reduce cyberattacks and maintain profitability. For this study, the definition of a small business is 500 or fewer employees (Small Business Association, 2019a). Eligibility for gender is irrelevant to the analysis and is not a criterion. The participants, small retail business owners who had expertise in the daily business activities, gave a definitive account of management strategies for countering potential cyberattacks.

I gained access to potential research participants from the U.S. Small Business Administration (SBA) online database, using the classification codes for retail businesses, located in the central region of Alabama. The district bureau of the U.S. SBA provides connections to the Dynamic Small Business Search website and the Small Business Size

Standards Table (SBA, 2019b). Gaining access to business owners and documentation to collect pertinent information about the potential participants is essential for the validity of the study (Yin, 2017). Once I gained approval from Walden’s Internal Review Board (IRB), the prospective participants received an invitational telephone call to seek their willingness to participate in a face-to-face interview. Access by telephone or face-to-face to a participant is essential to build trust and support in relationships (Irvine, Drew, & Sainsbury, 2013). Participants that were willing to participate received an invitation via email (see Appendix B) and a voluntary consent form to take part in a face-to-face interview and follow-up interviews for member checking. I provided a clear understanding of the subject matter for the study, the interview process, and the collection of data that enabled participants to understand the study focus and the phenomenon. I arranged a face-to-face interview with each participant at a convenient time and in a comfortable environment chosen by the participant.

Developing a working relationship with study participants is essential for success (Valipoor & Pati, 2016). I created a working relationship with the participants through efficient, ongoing contact throughout the research process and focused on my role as a researcher to the participant. I summarized the purpose and scope of the interview with emphasis on the problem statement and research questions during the initial contact with each participant. Additionally, I addressed the participants’ questions. I discussed the interview protocol as outlined in Appendix A. I manually transcribed the semistructured interview data within 48 hours from the conclusion and scheduled member checking with each participant to ensure the accuracy of my interpretations of the data collected. The value of the members checks is to add detailed data and saturate the data during qualitative research (Saunders et al., 2018). As the researcher, openness, integrity, and trustworthiness preservation is critical with the participants (Nadal et al., 2015). However, Rossetto (2014) warned researchers to carefully preserve boundaries to protect the relationship between the researcher and the participant and ethical obligations. I validated the interview data with each participant and enter the data into the qualitative analysis software tool QSR NVivo 12 to assist in coding material to identify themes.

Research Method and Design

Research Method

Qualitative research supports theory elaboration and theory generation instead of theory testing (Reinecke et al., 2016). I used a qualitative approach to explore strategies for maintaining the profitability of small businesses in the retail industry by reducing cyberattacks as this method was appropriate as a holistic framework for understanding the problem. Researchers using a quantitative method focus on applied and theoretical discoveries or findings that come from comprehensive research questions through a field study in natural conditions (Park & Park, 2016). Researchers use the quantitative method to examine variable relationships, differences, and causes of behavior through careful isolation, measurement, and evaluation of variables, focusing on predictability, process improvement, and control over time (Park & Park, 2016). I did not measure and evaluate variables’ relationships or differences, so a quantitative method was not suitable for this research study. Researchers using the mixed method approach combine qualitative and quantitative methods and often include multiple theoretical perspectives in their studies

(Hesse-Biber, 2015). A mixed method approach was not appropriate for this study because I did not include a quantitative component in my identification and exploration of successful strategies that some small business owners in the retail industry use to reduce cyberattacks to remain profitable.

Qualitative research is based on the understanding, by indicational data analysis, of observations that concentrate on facts or topics with a purpose that examines a problem's motives and actions in its real-world environment (Lewis, 2015; Yin, 2017). The qualitative methodology approach uses multiple sources of data collection and provides a better interpretation of the phenomenon, a more compelling and accurate explanation of the situation, and examination of the business problem (Hays, Wood, Dahl, & Kirk-Jenkins, 2016). A quantitative approach limits an understanding of the phenomenon while a qualitative approach involves the participants ' specific experiences (McCusker & Gunaydin, 2015). Technological advances allow researchers to access and analyze quantitative data and get results from large numbers quickly (Hochbein & Smeaton 2018). Starr (2014) described quantitative research as a statistical analysis of data. This study involved neither probability nor statistics; therefore, the quantitative approach was not a suitable choice. Usually, the data are converted to analysis text when spoken (Clark & Vealé, 2018). During semistructured interviews, I used the qualitative approach for this study to obtain insight and information from the participants through open dialog.

McCusker and Gunaydin (2015) noted that the mixed method approach provides a cumulative body of knowledge, which divides into several methodologies and therefore creates a deeper understanding of qualitative and quantitative data triangulation. However, the combined methodology is concerned with the issue, purpose, and context of research and may not provide the results with a holistic presentation of the phenomenon by quantitatively defined methodology (McCusker & Gunaydin 2015). Mixed approaches incorporate quantitative and qualitative analysis to answer the study problem. The use of mixed methods gives a more detailed view of the phenomenon than the use of just one method (McCusker & Gunaydin, 2015). The mixed method approach was not suitable for this study since a quantitative component was not necessary.

The research process consisted of qualitative analysis, a tool that documents thoughts, feelings, and experiences. A qualitative approach was selected because using qualitative analysis, as explained by Barnham (2015), is the best research method for gaining a more in-depth insight into behavior and drive. As the data may be digitized and synthesized, the way the data are processed is remarkable. The interpretation of information providing insight and patterning derives from quality data (Bansal, Smith, & Vaara, 2018). Yin (2017) described the qualitative method as a means of exploring the reality of a phenomenon that may be highly effective.

Research Design

Qualitative research designs include case studies, ethnographic, and phenomenological methods (Arino, Le Baron, & Milliken, 2016). This study was suitable for an exploratory study using a multiple case study design. To explore a real-life phenomenon in-depth and an environmental context, researchers use a case study design (Ridder, 2017). Zainal (2017) defined the strength of a case study as the ability to analyze and understand complex problems through contexts analysis; the case may be restrictive to a geographical area or population sample that may be small to large. Researchers use an ethnographical design to observe the cultural conduct of participants over a significant time, which was not the aim of this study (Baskerville & Myers, 2015). According to Arino et al. (2016), researchers use a phenomenological design to explore the meanings of the lived experiences of individuals to provide a first-person view. The purpose of this study was to obtain information on strategies for maintaining the profitability of small businesses in the retail industry by reducing cyberattacks, not to focus on the meanings of lived experiences of small business leaders. A phenomenological design was therefore not suitable for this study.

The selection of the correct study design was made possible by the consideration of three types of case studies designs for review. Pearson, Albon, and Hubball (2015) identified and summarized the three research designs that were explorative, explorative, and descriptive. An exploratory case study can facilitate a deep dive into the subject phenomena to help answer the research question and inform further research (Melewar, Foroudi, Dinnie, & Nguyen, 2017). The explanatory case analysis describes and determines associations and relationships between the case variables (Pearson et al., 2015). A concise case analysis offers a detailed contextual explanation of the case phenomena (Kaba, Baumann, Kolotylo, & Akhtar-Danesh, 2017). To choose the best design for a study , researchers must continue to examine the discrepancies between study designs.

Gentles, Charles, Ploeg, and McKibbon (2015) proposed the use of a single case study, provided that between four and 15 cases were for study purposes. Harrell (2017) and Weishäupl, Yasasin, and Schryen (2018) have cited cases as single and multiple loops, preferring single loop learning to respond quickly to cyberattacks. A multiple case study comprises several separately defined cases with comparative results from each case that help to conclude validity in findings (Gentles et al., 2017). A multiple case study design helps to define and understand the phenomenon in real-world environments employing document analysis and interviews to increase awareness and understanding of the problem in question in a limited context for the research question (Gentles et al. 2015). The use of a single case study did not support the purpose of my study. I selected a multiple case study to gain an in-depth description and understanding of the strategies that some small business owners in the retail sector use to reduce cyberattacks to remain profitable.

Population and Sampling

The population for the study was small retail business owners from the central region of Alabama. To understand the population, the SBA (2019c) defined businesses with 500 or fewer workers as small businesses. The targeted population for sampling included small retail business owners that are successfully using strategies that reduce cyberattacks to maintain profitability. I used purposeful sampling to identify participants within this population. Purposeful sampling is the method used by qualitative researchers to identify and select the studies that offer a wealth of useful knowledge on the phenomenon (Palinkas et al., 2015). A successful sample for a qualitative case study is enough if the participants know the phenomenon and topic of the study (Elo et al., 2014).

Purposeful sampling in qualitative research is often a solution to the practical constraints of time, resources, and access to information (Benoot, Hannes, & Bilsen, 2016). Researchers use a purposeful sample in qualitative data collection to identify participants with the necessary knowledge and experience to address the core research problem. The criteria for selecting the small business owners that participated in this study included: (a) participant's business meets the criteria established by the U.S. SBA specific to their North American Industry, classification system (NAICS) code dated 2019d or later; (b) had not had a cybersecurity breach in the last 18 months; (c) the central office resides within the Southeastern United States; and (d) has been in business for at least 3 years. Some successful small retail businesses with an effective cybersecurity plan investigation may be through the implementation of specific criteria.

Scholars share different perspectives on the appropriate number of participants in qualitative studies. There is a probability that only five participants can be adequate to achieve data saturation by sample size (Marshall & Rossman, 2016). Marshall and Rossman explained that the efficacy of the researcher in measuring the appropriate sample size correlates to data saturation. The primary aim of qualitative research is to ensure that the sample size is sufficiently small to handle the data and broad enough to provide a vibrant new understanding of the experience of participants (Fugard & Potts, 2015). In qualitative research, data saturation is achievable during the interview process, and the sample size is acceptable and complete (Fusch & Ness, 2015). Data saturation occurs when the added data collection does not include new themes (Ando, Cousins, & Young, 2014). I reached data saturation at the point when data collection activities did not give rise to any new themes or trends. I used an interview protocol (see Appendix A) to make sure all interviews are reliable. Additionally, I engaged every participant to test the accuracy of my interpretation of their responses.

Ethical Research

The priority was to conduct this study with the highest ethical conduct over and above reproach. Solicitation or requests for participants cannot occur before the approval by the IRB. Solicitation or requests for participation did not occur before the approval of the IRB was received. Ethical researchers seek permission from the IRB before participant recruitment and data gathering (Patton, 2002). The aim of the IRB committee is to protect against violations of human rights through a thorough examination of potential risks such as physical harm, emotional stress, or economic harm for participants (Bernard, 2013). Researchers must protect the privacy of participants and research partner organizations before, during, and after data collection (Sargeant, 2012).

I received approval from Walden University IRB with an approval reference number 04-15-20-0604773 before requesting study participants and collecting data. The informed consent process represents an important step in which participants must affirm in writing that they understand and agree to participate in all aspects of the research (Hardicre, 2014). In conducting research involving human subjects, qualitative researchers must follow ethical principles and communicate the scope of the study, the role of the researcher, and participant's expectations (Moustakas, 1994). I sent an e-mail to the prospective participants and an informed consent form. The informed consent form included the goal of the study, the research support organization, the perception of risks, and the volunteer aspect of the study. Cugini (2015) noted that informed consent is an essential function in the expectations of the participants in the study. Discussing data security, the exchange of results and the general essence of an interview is essential (Grady, 2015). I provided a preinterview orientation consisting of a review of the interview protocol, which informed the participant of the interview process and options for pause or withdrawal at any time. The effort to clarify and encourage the participant to interpret the consent form fosters an atmosphere in which the researcher can expand the conversation to help participants better understand their role in the research (Watts et al. 2016). If the participant wanted to withdraw, the destruction of all related data applicable to the participant was a requirement, and notification of such action sent to the participant through the U.S. Postal Service.

I secured and stored both paper and digital documents in a digital safe, which allows access to the required authentication with combination numbers. Digital data protection and the use of physical security procedures to store and secure hard copy documents in a locked office will ensure participants ' privacy and confidentiality rights (see Saunders, Kitzinger & Kitzinger, 2015). In addition, after 5 years of safeguarding, the last day of the month designated as the fifth year, destruction by fire of all forms, field notes, transcripts, and data collected will take place. Assigning unique identifiers is essential to preserving the confidentiality of the participants (Yin, 2017). I assigned a unique identifier to each participant. Externally, the use of participants ' data or privileged information was not permitted. Researchers must safeguard the confidentiality of the participants by using code names in a published study (Khan, 2014). I safeguarded the confidentiality of the research participants (RP) by using a unique coding system such as RP1, RP2, RP3, RP4, and RP5.

I informed each participant that the study was voluntary and that there are no consequences for withdrawing or not taking part. According to Hardicre (2014), it is necessary to remind participants that they participate voluntarily in a research study and that there are no repercussions for either withdrawal or not participating. I made participants aware that there are no advantages, incentives, or awards for study participation. A good motivator as a participant is to be interested in research directly or indirectly linked to the career of a person or potentially affects an organization (Lloyd & Hopkins, 2015). I reminded participants that their information is kept confidential and only aggregate data is published or shared with others.

Data Collection Instruments

The researcher is the primary instrument for collecting data (Yin, 2012). I was the primary method of collecting data for this research study. I used face-to-face semistructured interviews with open-ended questions. The interviews consisted of predetermined questions, as outlined in the Interview Protocol (see Appendix A). Data collection instruments may include a questionnaire, interview, or observation, and the researcher must question if the interview questions will add to the existing literature (Henderson, 2018). To strengthen and help the data collected in semistructured interviews, I reviewed and analyzed proprietary documents. I requested the participants to provide appropriate proprietary documents that may contain policies, training material, or related reports. Using documents, researchers can gain more insight into the subject matter and increase understanding of the topic (Siegner, Hagerman, & Kozak, 2018). Yin (2017) acknowledged various effective data collection methods, including interviews, digital recording, note-taking, evaluation, or peer-examination.

The face-to-face semistructured interview and observations with each participant provided data regarding experiences of cyberattacks and implemented managerial strategies of the business. Each participant shared specific experiences and strategies to combat cyberattacks. I promoted a relaxing atmosphere in which participants answered open-ended questions. McIntosh and Morse (2015) explained that participants need to be able to answer open-ended questions, and the researcher can probe their responses. Yin (2017) noted that researchers asked different research participants the same interview questions so that a range of responses and experiences would be possible. I used semistructured interviews to explore the strategies that some small retail business owners use to combat cyberattacks to remain profitable.

In the data collection process, I used member checking and methodological triangulation as a tool for quality control. Moussa (2015) indicated that researchers use member checking to enhance the reliability and legitimacy of qualitative research results. I used a digital recording device to record interviews with each participant's permission. I took detailed notes of the answers of all participants and transcribed the sessions to allow each participant to review for accuracy. Semistructured interview techniques are useful for mitigating bias because the researcher does not need to imply what the participant stated, instead, a researcher can ask for clarification of a question to obtain a clear and concise answer (Xu & Storr, 2012). I concentrated on the input of each participant until no new data emerged for collection.

The benefit of performing face-to-face interviews over online surveys or mail surveys is that during the interview, the participants can obtain clarification. Some of the drawbacks of carrying out face-to-face interviews include travel costs, possible participant embarrassment, and personal contact privacy violations (Yin, 2012). I used organizational documents and social media outlets to collect more participants' information. Documentation analysis and interview data improve the triangulation of data (Heale & Forbes, 2013). An advantage of researchers using documents to collect data is the opportunity to expand their findings. The downside of using records as a means of collecting additional information is that the collection of full documentation can be difficult for researchers (Yin 2012).

Data Collection Technique

I performed semistructured interviews for this qualitative multiple case study using an interview protocol (see Appendix A), together with member checking. Iivari (2018) contended that the participation of participants in the research process by checking and summarizing the answers to interview questions is significant. The researchers ' sequential questions allow the researcher to collect information effectively and achieve a better comparison of responses; also, the collection of data using more than one approach allows the researcher to interpret the phenomenon from different perspectives and to improve its validity (Iivari, 2018). Multiple data sources provide a clear snapshot of the experience in real life. I requested the participants to share any applicable proprietary documents that are relevant to this study for review.

Semistructured Interviews

Semistructured interviews were the first point in the data collection for this study. The participants were first contacted by telephone or e-mail to determine the level of interest in participation. All participants that were interested in participating in this study received a consent form and interview dates and times request. Participants were able to choose from a telephone interview or face-to-face interview based on location and availability. I adhered to the interview protocols by beginning the conversation with each participant with a review of the consent form. I reminded the participants of their option to withdraw from the conversation at any time (see Appendix A).

The reassurance of confidentiality and privacy was necessary for the participants. Interviews are one of the most common forms of data collection in qualitative research and require specific criteria such as documentation, archiving, and data validation (Rosenthal, 2016). After a semistructured interview, I asked participants to share any documents related to the topic for a document review.

Semistructured interviews have several advantages. Marshall and Rossman (2016) explained that semistructured interviews to be the single best way to collect data in qualitative studies. Yin (2018) has indicated that the use of semistructured interviews allows a person to focus on a specific subject, which is another benefit. One disadvantage of semistructured interviews is that the quality of the data obtained depends on the researchers ' capabilities (Yin, 2018).

Document Review

Document review includes using existing information to increase clarity on a subject (Yin, 2018). I asked the participants to provide any related material, like policies, training documents, or reports (public documentation), once the semistructured interviews are complete. Semistructured interview data, combined with the analysis and coding documents, revealed how small retail business owners use cyberattack prevention tactics to remain profitable. The document review has the advantage of extending the information and supporting data collected in other respects (Yin, 2018). The main disadvantage of a document review is that it is not always possible to access records that can be most helpful (Yin, 2018).

Data Saturation

Data saturation applies to qualitative research that uses interviews as the primary data source (Marshall & Rossman, 2016). I ensured data saturation by conducting follow-up interviews until there was no new data, and I reached a point of redundancy and acquired enough data for accurate analysis. Researchers should discontinue the interviewing process when participants cease to provide additional information on the subject (Lowe, Norris, Farris, & Babbage, 2018). Lowe et al. (2018) clarified that the researchers reached the goal of data saturation when interviews with the participants failed to produce new emerging themes.

Data Organization Technique

I organized the data collected using pseudonym codes to match the replies of participants. I then arranged the received data on an external hard disk and arranged the interview date in a digital folder. Bernard (2013) explained the process of organizing the collected data, which involved checking, maintaining, and reviewing the reflective journal throughout the study, inputting raw data into the qualitative data analysis software, and reviewing the researcher's notes. Pinfield, Cox, and Smith (2014) explained that data organization techniques involve data structure, storage, security, and data retrieval. Korhonen (2014) clarified that efficient data organization enables proper data storage and analysis to communicate research findings effectively.

I used Microsoft Word software to type the transcript for each recording interview. I provided a password-protected file for each participant, including a copy of the interview transcript. Researchers will create a specific file (Welch, Grossaint, Reid, & Walker, 2014) for each person. Once I had the participant's confirmation of interview results through member checking, the Microsoft Word transcription extraction occurred for the next action that was to import collected data into QSR NVivo 12 software. I coordinated and evaluated the responses of the participants using QSR NVivo 12 software. Edwards-Jones (2014) described QSR NVivo as a qualitative data analysis tool used to code, capture, and analyze data. All participants’ data for this qualitative case study, was imported into the QSR NVivo 12 software for thematic coding.

The use of codes to conceal participants ' identities guaranteed confidentiality. Bradley, Getrich, and Hannigan (2014) noted that the creation of a codebook with QSR NVivo allowed the organizing of data, narrative summaries, and cross-case analysis of interview data to address the research question. I ensured that the participants and their names were kept confidential by establishing a code that contained the letters RP, which are Research Participants, followed by the numbers 1 to 5. To access participant's data swiftly, I coded participants as RP1, RP2, RP3, RP4, and RP5.

Using reflective journals, qualitative researchers will build and organize their observations, perspectives, thoughts, and points of view as part of the research (Newington & Metcalfe, 2014). Appelbaum, Kogan, and Vasarhelyi (2017) explained that holding a self-reflective research paper is a technique that promotes reflection; researchers use their journal to define personal assumptions and objectives and to explain individual beliefs and subjectivities. To minimize researcher bias, I kept a journal to document personal reflections and observations that could potentially display any personal bias during the data collection process or add to the study. I did not choose participants with whom there was a business or personal relationship. The means of organizing and storing the transcribed responses of the participants involved the use of a password-protected external hard drive stored in a locked safe for 5 years. I am to destroy data after 5 years, by deleting computer files and burning all paper archives.

Data Analysis

The data analysis process involved the interpretation of the test results. The data analysis process involves preparing data for analysis, conducting a difference analysis, moving deeper and deeper into understanding the data, being the data, and interpreting the broader meaning of the data (Yin, 2018). Researchers gain an understanding of a qualitative phenomenon by discovering hidden trends, principles, and subjects in data analysis (Bedwell, McGowan, & Lavender, 2015; Gioia, Corley, & Hamilton, 2012). During data analysis, I used the conceptual framework of the actor-network theory as the prism. For data analysis, I used the five-step process of Yin (2018), data analysis for data collection, decomposition of data, reassembly of data, interpretation, and data conclusion.

During data analysis, scholars employed methodological triangulation to boost the quality and reliability of research findings (Rubin & Rubin, 2012). Renz, Carrington, and Badger (2018) noted that methodological triangulation is a way to enhance the analysis of quality data by crosschecking data from multiple sources. Researchers used statistical triangulation to assess data reliability and validity by combining knowledge from multiple sources (Carter, Bryant-Lukosius, DiCenso, Blythe, & Neville, 2014). I collected data using various methods, interview data with record data, and establish a clear case for topics with methodological triangulation.

Compiling Data

The first critical process of data collection is the cautious and methodical preparation of the initial data (Yin, 2018). I gathered data from the transcription of interviews and documentation using QSR NVivo 12 qualitative software. I read the text and listen to audio recordings to gain a deeper understanding of the data. Moustakas (1994) described epoch as a process to eliminate biases in research. Epoché aims to reserve the biases and interests of researchers to ensure the analysis is pure (Bazzano, 2014). Patton (2002) explained that epoché is the mechanism whereby a researcher adopts a phenomenological approach to prevent individual prejudice. During data reviews, I set aside my biases and ideology to minimize partiality.

Disassembling Data

Dismantling of data collected to smaller parts or sections occurs during the second stage of the analysis (Essary, 2014; Yin, 2018). Cox and McLeod (2014) explained that during the dismantling of the data, the themes emerge from data, keywords and, commonalities, which require coding. Researchers disassemble data by labeling and fragmentation (Yin, 2018). Yin (2018) discovered that the disassembly stage could repeat, considering the two-way flap between these compiling and disassembly steps, as part of a test and error process in code growth. In the disassembly method, I used the QSR NVivo 12 software. I coded and categorized data based on keywords and ideas in the literature review themes.

Reassembling Data

The third phase consists of data reassembly (Yin, 2018). The reassembly of the data is the stage in which study researchers reorganize the fragment or piece into various groupings and sequences within the original notes using important topics (Yin 2018). The method of assembly includes the clustering and grouping of labels into a group series (Yin, 2018). Researchers promote the rearrangement and combination of data by graphically representing or arraying it in lists and other tabular forms. The repeated analysis of the information helps to determine the presence of the same or different trends in the data (Baškarada, 2014; Yazan, 2015). I used the QSR NVivo 12 software to search, query, and visualization tools to identify links and patterns within and between categories to organize and reassemble information into themes. As new themes emerged, I created a new group and searched all the data to determine if I would use the original idea to code more data. Niedbalski and Ślęzak (2016) clarified that software from QSR NVivo had improved qualitative data analysis through the management and organization of data, ideas management, data query, and reporting.

Interpreting Data

The fourth step of Yin's (2018) five-phase is the reassembly of content to create a new narrative with corresponding tables and related graphics that become the critical analytical part of the study. The stage of interpretation occurs when the researcher creates narratives and conclusions from the reassembled data (Yin, 2018). The stage of interpretation includes the creation of stories from sequences and groups for results (Fusch & Ness, 2015). Essary (2014) proposed that researchers would find a deeper meaning throughout the interpretation stage. Researchers should consider how they empirically interpreted the data (Yin, 2018). As suggested by Marshall and Rossman (2016), the member verification process should look at a summary of the data interpretations of the participant. I engaged participants in member checking to verify the accuracy of the interview results.

Concluding Data

Yin (2018) noted that researchers would focus on the research findings. Compelling findings bring the whole analysis together (Yin, 2018). The findings of Yin (2018) relate to interpretation during the interpreting phases and through all other steps of the five-step data analysis process. The results must cover the importance of the data (Yazan, 2015). Cox and McLeod (2014) noted that data analysis findings included the results summary and tables to clarify outcomes.

Software Plan

A significant part of research projects is computer-aided qualitative data analysis (Davidson, Paulus & Jackson, 2016). Researchers use the QSR NVivo software to help code, organize, and position the data into topics (Edwards-Jones 2014). Researchers used QSR NVivo tools to review transcripts and help manage interviewed data (Bradley et al., 2015; Castleberry, 2014; Cridland et al., 2014). I used QSR NVivo's auto-coding feature to identify and relate similarities in data with proposals and emerging topics, and manually to review the data to determine consistency, search for accuracy and find topics within the data. I used Microsoft Word to note the answers to each interview recorded. I made available a password-protected file for each participant, which included a copy of the interview transcript, a participant summary, and a written endorsement.

Reliability and Validity

Reliability and validity are useful tools in the research process to provide findings that represent the data accurately. Kelly, Fitzsimons, and Baker (2016) have defined reliability as the degree to which research is reliable, stable, and repeatable. Trustworthiness means the replication of test results and validity indicates data accuracy (Yin, 2018). The study foundation is on reliability and validity, such as truth, value, consistency, neutrality, and applicability, so validity refers to integrity and reliability to consistency (Noble & Smith 2015). Multiple sources of data add value to research by providing a thorough account of the participants ' views of the phenomena. Methodological triangulation may include interviews, surveys, observations, and reviews of documents (Morgan, Pullon, Macdonald, McKinlay, & Gray, 2017). In this study, I used interviews and document reviews combined with member checking and triangulation to confirm the findings.

Reliability

The level of confidence in the results of a study is one of the researchers ' most critical concerns. Researchers can repeat a study when it comes to reliability (dependability) and establishes alignment with the objectivity and credibility of the study. Yin (2018) noted that member checking offers reliability within a qualitative framework. Cypress (2017) proposed that researchers can use the same methodology and research procedure to replicate a research design to address the same phenomenon when the research is reliable. The accuracy and quality of a research determination are by having an appropriate reliability strategy (Leung, 2015). I documented the steps and procedures in the interview protocol for this study (see Annex A). Reliability and dependability consisted of data interpretation inspections via member checking. The use of member checking techniques allows participants to act as co-interpreters to gain insight into both their corporate realities and the perspectives of the researchers in these realities (Iivari, 2018).

Validity

For validity or legitimacy, the reliability of the findings must be representative. Noble and Smith (2015) defined validity as the study's integrity and application, enabling the researchers to produce accurate results. Qualitative research validity refers to the sustainability of instruments, processes, and data (Leung, 2015). The researcher can conduct single-way testing by encouraging the participants to comment on the final transcript or answers to ensure that the knowledge represents the phenomenon equally (Noble & Smith, 2015). Research comparison and checks may use multiple data sources, such as archives and interviews (Canales 2015). I used interviews, member checks, and document reviews to accomplish these efforts. Qualitative analysis researchers incorporate in their studies credibility, confirmability and, transferability (Amankwaa, 2016). Credibility refers to how much research signifies the participant's point of view (Moon, Brewer, Januchowski-Hartley, Adams, & Blackman, 2016). Wayhuni (2012) explained that confirmability is the ability to adapt to the changing stability of the research project. Anney (2014) has clarified that the degrees to which the results of the study relate in such contexts, circumstances, periods, and populations are transferable. I used data triangulation to ensure that patterns and themes align with academic and business sources. Triangulation compares data from several sources to examine the quality of the results verification (Yin, 2018). I ensured that the participants had successfully implemented strategies to reduce cyberattacks to maintain profitability.

The reliability of the study findings is related to reliability (Twining, Heller, Nussbaum, & Tsai, 2017). I used methodological triangulation to view a single set of data from multiple perspectives. The methodological triangulation process consisted of interview data, document review, and membership checking. Member checking is a valuable credibility method. As a conventional method, Marshall and Rossman (2016) proposed e-mail follow-up interviews with clarity or elaboration issues. I provided the participants with the option to use either e-mail or face-to-face interviews for member checking. The participants in the study selected face-to-face member checking. I allowed each participant to review my analysis and my interview summary. I invited participants to confirm or add to my summary. Tracy (2010) explained that the members gain legitimacy through complete definition, triangulation, crystallization, and reflections.

Transferability included useful techniques to minimize the fiscal impact of cyberattacks on small retail businesses and refers to the findings to be applied in other settings or groups as defined by Noble and Smith (2015). In addition, Cope (2014) proposed transferability when a non-study participant would apply the results to his or her own experience. I used the interviews, insights, and participant feedback to improve the validity and transferability of the study to ensure that my results were relevant to my research question, and to encourage future research on strategies to combat small business cyberattacks.

Confirmability defines how the results relate to the research phenomenon (Yin, 2018). The participant reviews every interview for confirmation and guarantees the inquiry process ' validity (Hays et al., 2016). Confirmability relates to how the researcher demonstrates how the data represent the response of the participant and not the views of the actual researcher (Cope, 2014). I demonstrated confirmability by providing quotes and emerging themes. I reminded participants of the need to develop a comprehensive understanding of their responses, to recognize the themes needed to identify common themes extracted from their responses as factors contributing to the success of their business.

I gathered data through semistructured interviews, and a review of business documents engaged participants in member checking and continued to gather data until no new themes or patterns appeared. I continued to collect data until reaching data saturation. Fusch and Ness (2015) explained that data saturation occurs when no new evidence appears from interviews, and no new themes emerge from the collected data. Denzin (2012) suggested that the application of methodological triangulation could significantly improve data saturation capacity. The mixture of data sources helped to achieve data saturation. Triangulation leads to data saturation through the analysis of the different levels and points of view of the studied phenomenon, which ensures data diversity (Fusch & Ness, 2015).

Transition and Summary

In section 2, I provided the methodologies, tools, and techniques, planned for use in my study. I chose the use of a qualitative multiple case study to accomplish the stated research purpose. The section outlined details on the role of the researcher, participants, research method and design, population and sampling, ethical research, data collection instruments and technique, data organization technique, data analysis, reliability, and validity. In section 3, I will provide a presentation of findings, the implication to professional practice, and implication for social change, recommendations for action and further research, and my reflections.

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 some small business owners in the retail industry use to reduce cyberattacks to remain profitable. All research participants concluded that proactive security strategies were essential in alleviating data breaches. I administered six semistructured interview questions to each participant in a relaxed environment for each participant to provide detailed responses (see Appendix A). Through a combination of interview data, review of proprietary documents, comprehensive literature review, and conceptual framework, I discovered the strategies used by participants to protect their small retail business against cyberattacks, which include three themes: (a) business cybersecurity strategy, (b) network security, and (c) systems user access management. The results of the study support Von Bertalanffy's (1972) GST. In the following section of this report, I confirmed the relation between the themes described and extracted from the data collected and the conceptual framework.

Presentation of the Findings

The central research question was *What strategies do some small business owners in the retail industry use to reduce cyberattacks to remain profitable?* Five small business owners participated in the study. I examined a variety of theories in response to this question. I performed data analysis using thematic analysis and coding after the data collection process, transcript review, and completion of member checking. Moira and Brid (2017) explained that the researcher would recognize trends or common themes that provide valuable knowledge about the research question by utilizing thematic analysis of qualitative data. The three emergent themes were (a) business cybersecurity strategy, (b) network security, and (c) systems user access management. Von Bertalanffy's theory aligns with existing literature and themes generated in the findings.

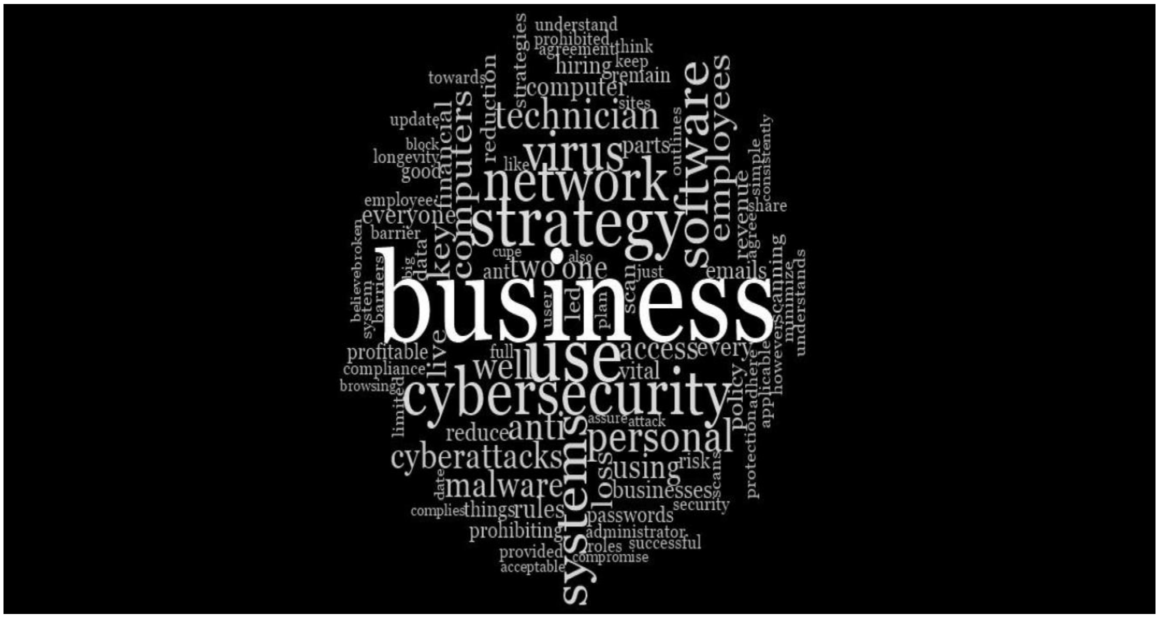

Figure 1. Word cloud of frequency query results for member-checked interviews.

Emergent Theme 1: Business Cybersecurity Strategy

The first theme that emerged from the data collection process was the need for small retail business owners to have a business cybersecurity strategy (see Table 1). After analyzing the responses of the participants, and inputting the data into QSR NVivo 12, it became evident that each participant regarded the cybersecurity strategy as a top priority. RP2 reported that there were no portions of the developed cybersecurity strategy that contributed to revenue loss. RP2 stated, “I have not had to deal with anything such as a data breach.” Additionally, RP2 stated, “All businesses should have a strategy.” RP3 stated, “I believe that it is in every business interest to have policies in place, no matter the size of business.” RP3 further stated, “We have not experienced a cyberattack, and we are confident in plans that are in place.” RP4 stated, “The only thing that I can say is that every business needs a plan of action.” Additionally, RP4 stated, “I have not experienced any deficiency in my current business strategy.” Table 1 shows the frequency of participants’ comments concerning cybersecurity strategies.

Table 1

Number of Times Business Cybersecurity Strategy Discussed

Theme 1 Business cybersecurity strategy	*n*	Percentage of contribution to the emergent theme
RP1	8	19%
RP2	8	19%
RP3	11	26%
RP4	9	21%
RP5	7	15%
	43	100%

Note. *n* = frequency or number of coding references

The findings collected from small retail business owners are in line with the conceptual framework and the literature review in the following ways: (a) recognizing that a business is composed of several subsystems, (b) reasons to implement a cybersecurity strategy within the business strategy, and (c) understanding the financial impact of cyberattacks. Theme 1 aligned with Ajayi's findings (2016) in that business environments is composed of internal and external systems that work together differently to create a positive impact on business operations. Ajayi explained that small business owners need to consider the effect on business operations of both internal and external influences, which contributes to business success. Sallos, Garcia-Perez, Bedford, and Orlando (2019) explained that a knowledge-based perspective could serve as an appropriate forum for a phenomenon-based view of organizational cybersecurity. Theme 1 relates to von Bertalanffy's (1972) GST because the interconnection between the components of a system is essential when compared to the components themselves. Boiko, Shendryk, and Boiko (2019) clarified that the approach used by business leaders to coordinate threats associated with cybersecurity and their essential operations is a vital cybersecurity strategy. I reviewed participant interviews and proprietary documents. All five participants emphasized the importance of an effective cybersecurity strategy. Strategic planning is a deliberate strategy by business owners to recognize reasonable threats, disruptions, and opportunities for their businesses (Kachaner, King, &Stewart, 2016). The implications of these findings are focused on the interconnectedness of the expectations and activities of a business cybersecurity strategy that permits small retail owners to remain profitable.

Emergent Theme 2: Network Security

The second theme that emerged during data analysis was network security. The small retail owners' second priority was related to technology and methods to protect their network. The method comprises inspecting network traffic using (a) network inspection technologies, (b) executing a network security system to implement security policies to respond to threats identified by network inspections, and (c) adaptively reassessing security policies based on the evolution of technology. Antivirus software manifested as evidence for an effective strategy for securing data and the network. Risks, threats, and attacks from computer viruses and malware mitigation are by using antivirus software as protection. RP2 stated, “I use live scan antivirus and malware software that is consistently updated.” RP4 stated, “I ensure that all my system networks have the most up to date antivirus software, and instead of waiting for weekly scans, my systems are set up to scan every 24 hours.” RP5 stated, “I like to use a live scan antivirus software that can also detect malware.” To check and validate the interview data, I reviewed a variety of business documents to engage in methodological triangulation.

The participants had different network security plans that were different in delivery, but similar in content. RP1 and RP3 claimed that having a computer system and network technician is key to a cybersecurity strategy. RP1 stated, “I have a technician that keeps all of my network and computers updated.” RP3 unique business affiliation helps to ensure that the network is protected, “We are entitled to the latest antivirus software available.” The small retail owners were most concerned with protecting their local data. A key point in this study was that the participants did not view the threat from malware as more or less severe than any other cybersecurity threat. Although technology solutions played a crucial role in safeguarding business assets, information security users often formed the weakest link. The ability to manage and guide information security behaviors of employees was found to be a new challenge for the participants. Budzak (2016) explained that the behavior of users becomes a threat to information security. Table 2 shows the frequency of participants’ comments concerning network security.

Table 2

Number of Times Network Security Discussed

Theme-2 Network security	*n*	Percentage of contribution to the emergent theme
RP1	6	17%
RP2	9	26%
RP3	7	20%
RP4	5	14%
RP5	8	23%
	35	100%

Note. *n* = frequency or number of coding references

The current function of antivirus and malware software does not adequately address data and network security concerns for these small retail business owners. Information of how these small business retail owners protected their business data from cyberattacks were presented in the reviewed network protection documents. Based on the analysis, participants were continuously improving their network security policy to protect business data against cyberattacks. According to von Bertalanffy (1968), open systems and systems thinking are at the center of general system theory. Open systems communicate to either adjust or predict the best fit for their environment (Panda & Kapoor, 2017). The participants concluded that investing in an experienced network technician or the most updated antivirus software available is vital for protecting a business network infrastructure. RP1 stated, “Get a good computer technician” RP5 stated, “Buy the software or risk being sued.” The strategy aligned with the analysis of

Silvia (2015), who explained that understanding business practices is critical to adopt new ideas and behaviors.

Emergent Theme 3: Systems User Access Management

The third theme that emerged during data analysis was systems user access management. All participants had strong policies that supported their overarching cybersecurity strategy. Calopa (2017) explained that strategies such as policies and strategic management are essential to small business success. The results from analyzing the user agreement that each owner provided supported the findings whereby the business owners recognized and measured data risk and established a cost-benefit analysis of possible mitigation. RP1 hired a network technician to monitor the abuse of systems. However, RP1 confirms the full compliance of the system user access policy, “I assure [*sic*] the compliance of my staff.” RP2 stated, “We limited the access to specific data, and our computers are only used for business transactions.” RP3 stated, “Employees are not allowed to use our system to access personal emails.” Additionally, RP3 stated, “They are assigned business emails to use at work, and administration has access to all business emails.” RP4 stated, “Visiting prohibited sites are against the rules, and no one uses the business computers to access personal information.” RP5 stated, “I have seen so many big businesses lose money and customers because someone broke into their database. I learned from that…what we do here is minimize the use of business computers for personal use.” Table 3 shows the frequency of participants’ comments concerning systems user access management.

Table 3

Number of Times Systems User Access Management Discussed

Theme-3 Systems user access management	*n*	Percentage of contribution to the emergent theme
RP1	13	25%
RP2	11	21%
RP3	6	11%
RP4	9	17%
RP5	14	26%
	53	100%

Note. *n* = frequency or number of coding references

Participants confirmed the employee's agreement to their system user access policy by requiring each employee to sign a system user agreement as a management tool. The results were consistent with the findings of Kure, Islam, and Razzaque (2018), who identified cybersecurity risk management as a fundamental and critical mechanism for managing data breach risks. The participants used the system user agreement as a tool to identify, assess, and mitigate the risk associated with the availability, confidentiality, integrity of their business, and customers' data. RP2 stated, "Each employee signs a user agreement when hired as an employee" RP3 stated, "All employers have read and signed that they understand our business policies." RP4 stated, "Everyone complies with the rules…my network security policy using our business systems for personal use is strictly prohibited." Paliszkiewicz (2019) explained that information or data may take different forms, such as electronic or physical information, for leaders to concentrate on adequate protection of data security while maintaining a focus on successful policy execution. The policy applied to all system administrators, network administrators, and operators who are responsible for security of all data and application that are essential to business operations.

The participants believed that they had addressed much of their cybersecurity risks by implementing solid policies that support the cybersecurity strategy. Cybersecurity is a vital component of small business systems (Atoum & Otoom, 2016). The findings relate to von Bertalanffy’s (1972) GST because the participants shared the development and implementation of strategies to mitigate cybertheft of PII and for supporting the overall functioning of other organizational systems within small retail businesses.

Applications to Professional Practice

The findings of this study are important for developing approaches that are used by small retail business owners to reduce cyberattacks to remain profitable. I revealed three major themes shared by five small retail owners in the southeastern region of the U.S. who successfully reduced cyberattacks and remained profitable. New or existing small retail owners may establish new strategies by applying the findings from this study to contribute to an effective cybersecurity infrastructure. The possibility of a small business cyberattack is increased by small business owners failing to measure and address their internal cybersecurity posture (Williams, Levi, Burnap, & Gundur, 2019). The small retail owners of this study had adequate support structures, access to trusted sources of information on cybersecurity, and they were confident in their strategies to reduce cyberattacks to remain profitable.

The findings of the study may provide current and potential small business owners with an overview of successful cybersecurity approaches as well as areas on which they can concentrate their attention. The application to professional practice could include encouraging small retail business owners to implement new approaches that will promote enhanced steps that will reduce cyberattacks to remain profitable. Potential researchers could use the findings of this study to form the basis of future recommendations for the development of a small business cybersecurity strategy as well as further potential studies.

Implications for Social Change

The primary implications for positive social change may be through small retail business owners applying strategies that enable the potential to reduce cyberattacks to remain profitable. Small business owners need to remain profitable to create new employment opportunities to help alleviate poverty in communities and improve the economy from the revenue created by new jobs. The profitability success of small retail owners may also have multiple impacts on other stakeholders such as product and service providers, and their success may contribute to the promotion of other social activities (Lee, 2018). Mitchell, Madil, and Chreim (2015) encouraged business leaders to carry out social initiatives such as social entrepreneurship and social marketing that create positive social impact and economic benefit and contribute to improving local community well-being.

The implications for social change include the potential for small retail business owners to mitigate cybertheft of PII, subsequently increasing consumer confidence and improving the financial stability of small retail businesses to create economic growth in local communities. By establishing a business cybersecurity strategy and managing information security risks, business owners can potentially focus their efforts on protecting information assets and resources. Small business owners may use study findings to increase awareness of cybersecurity and enhance their local business cybersecurity culture and beyond. Many societies can benefit because small business owners may reach other than their peer network and influence those responsible for the implementation of cybersecurity strategies to reduce cyberattacks. Continued efforts by business owners may significantly increase profitability and foster a healthy culture of cybersecurity beyond the local communities they represent.

Recommendations for Action

The purpose of this qualitative multiple case study was to explore the strategies that some small business owners in the retail industry use to reduce cyberattacks to remain profitable. The research findings include three major themes. The action recommendations include small retail owners implementing strategies to reduce cyberattacks, improve business networks, and efficiently manage access to systems. Small retail business owners and future entrepreneurs should explore the findings of this research study to implement strategies to reduce cyberattacks to remain profitable. The results of this study indicated that the revenue and profits of small retail owners who were effective in reducing cyberattacks increased.

The findings of this study are invaluable to small business owners in battling cyberattacks and staying profitable. Dissemination of these findings for small retail business owners will promote their cybersecurity strategies. Rose and Flynn (2018) explained that researchers must disseminate research findings to influence policies and managerial practices. This study will later be available for review by scholars, business owners, and students in the ProQuest database. I will provide all participants with a summary of the findings and recommendations. I will also be willing to discuss the results at academic conferences, forums for small business owners, and conferences on leadership. I plan to publish a journal article to reach other people who may be interested in my study.

Recommendations for Further Research

The findings of this study warrant further research, due to the substantial contributions of small retail business owners to the U.S. economy and their support within their community. Park and Campbell (2018) clarified that small business owners are important stakeholders, and they are invaluable in their philanthropic service to their local communities. This research was limited to small retail owners in the southeastern region of the U.S. Greener (2018) explained that limitations allow researchers to identify and recommend future research topics. The sample size limited the study and restricted the transferability of the findings. My recommendation is to have a greater number of participants from various geographic locations, in addition to the U.S. Southeast region. The sample size for this study was adequate to attain saturation; however, future researchers may consider using a larger sample.

Future researchers may identify additional areas to research by focusing on the emergent themes of the study including, (a) business cybersecurity strategy, (b) network security, and (c) systems user access management. Additionally, researchers may use different theories, methodologies, and designs to gather and analyze participant data to explore the strategies that some small business owners in the retail industry use to reduce cyberattacks to remain profitable. Finally, to understand failure and recovery, potential researchers may plan to explore the inverse of this study and analyze successful cyberattacks that reduce profitability for small businesses.

Reflections

The Doctor of Business Administration (DBA) program at Walden University has allowed me to value time management, persistence, self-discipline, and focus. I have acquired considerable knowledge of the challenges of cybersecurity for small businesses and on some successful strategies implemented by small retail owners to remain profitable. The analysis and effect of cyberattacks on small retail businesses were informative and helpful in understanding effective cybersecurity business strategies that lead to success. Knowledge sharing is one way of strengthening our culture.

The research process never ends and can create challenges for an analyst. I was grateful for the five successful small business owners with cybersecurity strategies that enable small businesses to remain profitable. The participants were eager to participate in this research without the influence of the probability of personal prejudices or preconceived values. I believe that the experience and knowledge gained, coupled with the results of this study, will be useful and positive for my future as a scholar-researcher. I remain motivated with the desire to extend my research on small businesses after the completion of this program. Achieving a doctorate's high academic expectations is a daunting and frustrating path, but it is rewarding to learn more about one's perseverance, dedication, and tenacity in completing the doctoral journey.

Conclusion

I used a qualitative multiple case study to explore the strategies that some small business owners in the retail industry use to reduce cyberattacks to remain profitable. Five small retail owners located in the state of Alabama who had the expertise and successfully implemented a business cybersecurity strategy participated in this research. I collected data using methodological triangulation until reaching data saturation. Data analysis consisted of the use of QSR NVivo 12, recorded transcripts, and member checking to confirm the participants' accurate responses.

The findings of this study revealed three effective strategies that small retail business owners use to reduce cyberattacks to remain profitable. The three strategies focused on the: (a) business cybersecurity strategy, (b) network security, and (c) systems user access management. Current small retail owners and potential entrepreneurs can benefit from the findings of this study to learn about successful strategies that help reduce cyberattacks and expand these strategies to remain profitable. The findings may also help foster positive social change by helping small retailers reduce PII Internet fraud, thereby improve customer trust and improve small retail businesses' financial stability to build economic prosperity in the local community.

References

Ablon, L., & Libicki, M. (2015). Hacker's bazaar: The markets for cybercrime tools and stolen data. *Defense Counsel Journal., 82*, 143-152. doi:10.12690/0161-8202-82.2.143

Afriyie, S. O., Kong, Y., Danso, P. O., Ibn Musah, A. A., & Akomeah, M. O. (2019). Do corporate governance mechanisms and internal control systems matter in reducing mortality rates? *International Journal of Health Planning and Management, 34,* 744-760. doi:10.1002/hpm.2732

Aguilar, L. A. (2015). *The need for greater focus on the cybersecurity challenges facing small and midsize businesses.* U.S. Securities and Exchange Commission. Retrieved from https://www.sec.gov

Agyei-Mensah, B. K. (2016). Internal control information disclosure and corporate governance: Evidence from an emerging market. *Corporate Governance: The International Journal of Business in Society, 16*(1), 79-95. doi:10.1108/cg-10-2015-0136

Ajayi, A. (2016). Impact of external business environment on organizational performance of small and medium scale enterprises in Osun State, Nigeria. *Scholedge International Journal of Business Policy & Governance, 3*, 155-166. doi:10.19085/journal.sijbpg031002

Alter, S. (2018). System interaction theory: Describing interactions between work systems. *Communications of the Association for Information Systems, 42*, 233-267. doi:10.17705/1CAIS.04209

Amankwa, L. (2016). Creating protocols for trustworthiness in qualitative research. *Journal of Cultural Diversity, 23*, 121-127. Retrieved from http://www.tuckerpub.com/jcd.htm

Andersson Schwarz, J., & Burkart, P. (2015). Piracy and social change. *Popular Communication, 13*, 1-5. doi:10.1080/15405702.2015.990329

Ando, H., Cousins, R., & Young, C. (2014). Achieving saturation in thematic analysis: Development and refinement of a codebook. *Comprehensive Psychology, 3*, 03-CP. doi:10.2466/03.CP.3.4

Anney, V. (2014). Ensuring the quality of the findings of qualitative research: Looking at trustworthiness criteria. *Journal of Emerging Trends in Educational Research and Policy Studies, 5*, 272-281. Retrieved from http://jeteraps.scholarlinkresearch.com

Appelbaum, D., Kogan, A., & Vasarhelyi, M. A. (2017). An introduction to data analysis for auditors and accountants. *CPA Journal*, *87*(2), 32-37. Retrieved from http://www.cpajournal.com/

Arief, B., Bin Adzmi, M. A., & Gross, T. (2015). Understanding cybercrime from its stakeholders' perspectives: Part1-attackers. *IEEE Security & Privacy, 13*, 71-76. doi:10.1109/MSP.2015.19

Arino, A., LeBaron, C., & Milliken, F. J. (2016). Publishing qualitative research in academy of management discoveries. *Academy of Management Discoveries, 2,* 109-113. doi:10.5465/amd.2016.0034

Arouri, M., & Pijourlet, G. J. (2017). CSR performance and the value of cash holdings: International evidence. *Journal of Business Ethics, 140*, 263-284. doi:10.1007/s10551-015-2658-5

Ashenmacher, G. (2016). Indignity: Redefining the harm caused by data breaches. *Wake Forest Law Review, 51*, 1. Retrieved from http://lawreview.law.wfu.edu/

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

Au, M. H., Liang, K., Liu, J. K., Lu, R., & Ning, J. (2018). Privacy-preserving personal data operation on mobile cloud-chances and challenges over advanced persistent threat. *Future Generation Computer Systems, 79*, 337-349. doi:10.1016/j.future.2017.06.021

Bansal, P., Smith, W. K., & Vaara, E. (2018). New ways of seeing through qualitative research. *Academy of Management Journal, 61*, 1189-1195. doi:10.5465/amj.2018.4004

Barafort, B., Mesquida, A. L., & Mas, A. (2017). Integrating risk management in IT settings from ISO standards and management systems perspectives. *Computer Standards & Interfaces, 54*, 176-185. doi:10.1016/j.csi.2016.11.010

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

Baškarada, S. (2014). Qualitative case study guidelines. *Qualitative Report, 19*(40), 1-25. Retrieved from http://www.nova.edu/ssss/QR/index.html

Baskerville, R. L., & Myers, M. D. (2015). Design ethnography in information systems. *Information Systems Journal, 25*(1), 23-46. doi:10.1111/isj.12055

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information & 122 Management*, *51*, 138-151. doi:10.1016/j.im/2013.11.004

Bauer, A. M. (2016). Tax avoidance and the implications of weak internal controls. *Contemporary Accounting Research, 33,* 449-486. doi:10.1111/1911-3846.12151

Bazzano, M. (2014). On becoming no one: Phenomenological and empiricist contributions to the person-centered approach. *Person-Centered & Experiential Psychotherapies, 13,* 250-258. doi:10.1080/14779757.2013.804649

Beckett, P. (2015). An intelligent approach to security. *Network Security, 2015*(2), 18-20. doi:10.1016/S1353-4858(15)30009-X

Bedwell, C., McGowan, L., & Lavender, D. T. (2015). Factors affecting midwives' confidence in intrapartum care: A phenomenological study. *Midwifery, 31,* 170-176. doi:10.1016/j.midw.2014.08.004

Bell, S. (2017). Cybersecurity is not just a 'big business' issue. *Governance Directions, 69,* 536-539. Retrieved from https://trove.nla.gov.au

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

Bentley-Goode, K. A., Newton, N. J., & Thompson, A. M. (2017). Business strategy, internal control over financial reporting, and audit reporting quality. *Auditing: A Journal of Practice & Theory, 36*, 49-69. doi:10.2308/ajpt-51693

Benton, D. C., González-Jurado, M. A., Beneit-Montesinos, J. V., & Fernández, M. P. F. (2013). Use of open systems theory to describe regulatory trends. *Journal of Nursing Regulation, 4*(3), 49-56. doi.10.1016/S2155-8256(15)30131-9

Bernard, H. R. (2013). *Social research methods: Qualitative and quantitative approaches* (2nd ed.). Thousand Oaks, CA: Sage.

Bosse, D. A., & Phillips, R. A. (2016). Agency theory and bounded self interest. *Academy of Management Review, 41*, 279-297. doi:10.5465/amr.2013.0420

Boiko, A., Shendryk, V., & Boiko, O. (2019). Information systems for supply chain management: Uncertainties, risks, and cybersecurity. *Procedia Computer Science, 149*, 65-70. doi:10.1016/j.procs.2019.01.108

Bradley, P. V., Getrich, C. M., & Hannigan, G. G. (2015). New Mexico practitioners' access to and satisfaction with online clinical information resources: An interview study using qualitative data analysis software. *Journal of the Medical Library Association, 103*, 31-35. doi:10.3163/1536-5050.103.1.006

Brahmana, R. K., Brahmana, R. K., & Fei Ho, T. C. (2018). Training and development policy, corporate governance, and firm performance. *Gadjah Mada International Journal of Business, 20*, 59-87. doi:10.22146/gamaijb.12995

Brown, H. S. (2016). After the data breach: Managing the crisis and mitigating the impact. *Journal of Business Continuity & Emergency Planning, 9*, 317-328. Retrieved from https://www.ncbi.nlm.nih.gov

Burnap, P., French, R., Turner, F., & Jones, K. (2018). Malware classification using self organising feature maps and machine activity data. *Computers & Security, 73*, 399-410. doi:10.1016/j.cose.2017.11.016

Buyya, R., Srirama, S. N., Casale, G., Calheiros, R., Simmhan, Y., Varghese, B., & Toosi, A. N. (2018). A manifesto for future generation cloud computing: Research directions for the decade. *ACM computing surveys (CSUR), 51*(5), 1-38. doi:10.1145/3241737

Cabaj, K., Kotulski, Z., Ksiezopolski, B., & Mazurczyk, W. (2018). Cybersecurity: Trends, issues, and challenges. *EURASIP Journal on Information Security, 10*(1), 1-3. doi:10.1186/s13635-018-0080-0

Calvard, T. S., & Jeske, D. (2018). Developing human resource data risk management in the age of big data. *International Journal of Information Management, 43*, 159-164. doi:10.1016/j.ijinfomgt.2018.07.011

Canales, P. (2012). Complexity theory in political science and public policy. *Political Studies Review, 10,* 346-358. doi:10.1111/j.1478-9302.2012.00270.x

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

Castleberry, A. (2014). NVivo 10 [software program]. Version 10. QSR International, 2012. *American Journal of Pharmaceutical Education, 78,* 25-26. doi:10.5688/ajpe78125

Central Intelligence Agency. (2015). *The world fact book: Internet users.* Retrieved from https://www.cia.gov/index.html

Chaudhary, R., Kumar, N., & Zeadally, S. (2017). Network service chaining in fog and cloud computing for the 5G environment: Data management and security challenges. *IEEE Communications Magazine, 55*(11), 114-122. doi:10.1109/MCOM.2017.1700102

Cheng, L., Liu, F., & Yao, D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 7,* e1211. doi:10.1002/widm.1211

Christoffersen, M. G. (2018). Risk, danger, and trust: refining the relational theory of risk. *Journal of Risk Research, 21*, 1233-1247. doi:10.1080/13669877.2017.1301538

Clark, K. R., & Vealé, B. L. (2018). Strategies to enhance data collection and analysis in qualitative research. *Radiologic Technology, 89*, 482-485. Retrieved from http://www.radiologictechnology.org

Collier, R. (2016). The Obama administration and incident response: A report. *Information & Security, 34*, 105-120. doi:10.11610/isij.3408

Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: Risks, vulnerabilities, and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research, 6*, 31-38. doi:10.19101/IJACR.2016.623006

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

Copeland, M. (2017). Cybersecurity: How security vulnerabilities affect your business. *Cyber Security on Azure,* 3-31. doi:10.1007/978-1-4842-2740-4_1

Cosenz, F., & Noto, G. (2018). A dynamic business modelling approach to design and experiment new business venture strategies. *Long Range Planning, 51*, 127-140. doi:10.1016/j.lrp.2017.07.001

Cox, D. D., & McLeod, S. (2014). Social media marketing and communications strategies for school superintendents. *Journal of Educational Administration, 52*, 850-868. doi:10.1108/JEA-11-2012-0117

Cozzolino, A., Verona, G., & Rothaermel, F. T. (2018). Unpacking the disruption process: New technology, business models, and incumbent adaption. *Journal of Management Studies, 55,* 1166-1202. doi:10.1111/joms.12352

Cridland, E. K., Jones, S. C., Caputi, P., & Magee, C. A. (2014). Qualitative research with families living with autism spectrum disorder: Recommendations for conducting semistructured interviews. *Journal of Intellectual and Developmental Disability, 40*, 78-91. doi:10.3109/13668250.2014.964191

Cugini, M. (2015). Successfully navigating the human subjects approval process. *Journal of Dental Hygiene, 89,* 54-46. Retrieved from http://jdh.adha.org

Cypress, B. S. (2017). Rigor or reliability and validity in qualitative research: Perspectives, strategies, reconceptualization, and recommendations. *Dimensions of Critical Care Nursing, 36*, 253-263. doi:10.1097/DCC.0000000000000253

D'Arcy, L., & Lowry, P. B. (2019). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information System Journal*, *29*, 43-69. doi:10.1111/isj.12173

Davidson, J., Paulus, T., & Jackson, K. (2016). Speculating on the future of digital tools for qualitative research. *Qualitative Inquiry, 22*, 606-610. doi:10.1177/1077800415622505

Dawson, M., Dawson, M., Eltayeb, M., & Omar, M. (2016). *Security Solutions for Hyperconnectivity and the Internet of Things.* IGI Global.

Denzin, K. N. (2012). Triangulation 2.0. *Journal of Mixed Methods Research, 6*, 80-88. doi:10.1177/1558689812437186

Ding, D., Han, Q. L., Xiang, Y., Ge, X., & Zhang, X. M. (2018). A survey on security control and attack detection for industrial cyber-physical systems. *Neurocomputing, 275*, 1674-1683. doi:10.1016/j.neucom.2017.10.009

Douglass M., Garbaye R., & Ho, K.C. (2019). The rise of progressive cities east and west. In: Douglass M., Garbaye R., Ho K. (Eds.), *The Rise of Progressive Cities East and West Series: Vol. 6. ARI - Springer Asia Series:* (pp. 3-21). doi:10.1007/978-981-13-0209-1-1

Drack, M., & Schwarz, G. (2010). Recent developments in general system theory. *Systems Research & Behavioral Science, 27,* 601-610. doi:10.1002/sres.1013

Eddolls, M. (2016). Making cybercrime prevention the highest priority. *Network Security, 2016*(8), 5-8. doi:10.1016/S1353-4858(16)30075-7

Edwards-Jones, A. (2014). Qualitative data analysis with NVIVO. *Journal of Education for Teaching, 40,* 193-195. doi:10.1080/02607476.2013.866724

Elo, S., Kääriäinen, M., Kanste, O., Pölkki, T., Utriainen, K., & Kyngäs, H. (2014). Qualitative content analysis: A focus on trustworthiness. *Sage Open, 4*(1), 1-10. doi:10.1177/2158244014522633

Essary, M. L. (2014). Key external factors influencing successful distance education programs. *Academy of Educational Leadership Journal, 18,* 121-136. Retrieved from http://www.alliedacademies.org

Federal Emergency Management Agency [FEMA]. (2018). *Be prepared for a cyberattack.* Washington, DC. Retrieved from https://www.fema.gov

Fink, L., Yogev, N., & Even, A. (2017). Business intelligence and organizational learning: An empirical investigation of value creation processes. *Information & Management, 54,* 38-56. doi:10.1016/j.im.2016.03.009

Flores, W., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers and Security, 59*, 26-44. doi:10.1016/j.cose.2016.01.004

Frazer, L. (2016). Internal control: Is it a benefit or fad to small companies? A literature dependency perspective. *Journal of Accounting and Finance, 16*(4), 149-161. doi:10.33423/jaf.v16i4.1047

Fugard, A. J., & Potts, H. W. (2015). Supporting thinking on sample sizes for thematic analyses: A quantitative tool. *International Journal of Social Research Methodology, 18*, 669-684. doi:10.1080/13645579.2015.1005453

Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report, 20*, 1408-1416. Retrieved from http://www.nsuworks.nova.edu

Gal, G., Länsiluoto, A., Jokipii, A., & Eklund, T. (2016). Internal control effectiveness-a clustering approach. *Managerial Auditing Journal, 31*, 5-34. doi:10.1108/MAJ-08-2013-0910

Gao, X., & Jia, Y. (2016). Internal control over financial reporting and the safeguarding of corporate resources: Evidence from the value of cash holdings. *Contemporary Accounting Research, 33*, 783-814. doi:10.1111/1911-3846.12164

García, J. A. T., Skotnicka, A. G., & Zamora, D. T. (2015). The new technology-based firm profile required for a delimitation of its definition in empirical studies. *International Journal of Engineering Management and Economics, 5*(1-2), 114-128. doi:10.1504/IJEME.2015.069903

George, G. (2016). Management research in AMJ: Celebrating impact while striving for more. *Academy of Management Journal, 59*, 1869-1877. doi:10.5465/amj.2016.4006

Gepp, A., Linnenluecke, M. K. Terrence, J. O., & Smith, T. (2018). Big data techniques in auditing research and practice: Current trends and future opportunities. *Journal of Accounting Literature, 40*, 102-115. doi:10.1016/j.acclit.2017.05.003

Gentles, S. J., Charles, C., Ploeg, J., & McKibbon, K. A. (2015). Sampling in qualitative research: Insights from an overview of the methods literature. *Qualitative Report, 20*(11), 1772-1789. Retrieved from https://pdfs.semanticscholar.org

Ghourab, E. M., Azab, M., & Mansour, A. (2019). Spatiotemporal diversification by moving-target defense through benign employment of false-data injection for dynamic, secure cognitive radio network. *Journal of Network & Computer Applications*, *138*, 1-14. doi:10.1016/j.jnca.2019.02.020

Giboney, J. S., Proudfoot, J. G., Goel, S., & Valacich, J. S. (2016). The security expertise assessment measure (SEAM): Developing a scale for hacker expertise. *Computers & Security, 60,* 37-51. doi:10.1016/j.cose.2016.04.001

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2012). Seeking qualitative rigor in inductive research notes on the Gioia methodology. *Organizational Research Methods, 16*, 15-31. doi:10.1177/1094428112452151

Goldsborough, R. (2016). Protecting yourself from ransomware. *Teacher Librarian*, *43*(4), 70-71. Retrieved from http://www.teacherlibrarian.com

Grace, K., Vincent, M., & Evans, A. (2018). Corporate governance and performance of financial institutions in Kenya. *Academy of Strategic Management Journal, 17*(1), 1-13. Retrieved from http://www.abacademies.org/journals/academy-of-strategic-management-journal-home.html

Grady, C. (2015). Enduring and emerging challenges of informed consent. *New England Journal of Medicine, 372,* 855-862. doi:10.1056/nejmc1503813

Graves, J. (2017). Data flow management: Why and how. *Network Security, 2017*(1), 5-6. doi:10.1016/S1353-4858(17)30004-1

Greene, J., Gupta, R., L'Helias, S., & McCracken, B. (2017). The role of corporate boards: A roundtable discussion of where we're going and where we've been. *Journal of Applied Corporate Finance, 29,* 22-35. doi:10.1111/jacf.12218

Greener, S. (2018). Research limitations: the need for honesty and common sense. *Interactive Learning Environments, 26*, 567-568. doi:10.1080/10494820.2018.1486785

Grosz, B. J., & Stone, P. (2018). A century-long commitment to assessing artificial intelligence and its impact on society. *Communications of the ACM, 61*, 68-73. doi:10.1145/3198470

Gwebu, K. L., Jing, W., & Li, W. (2018). The role of corporate reputation and crisis response strategies in data breach management. *Journal of Management Information, 35*(2), 683-714. doi:10.1080/07421222.2018.1451962

Hajisalem, V., & Babaie, S. (2018). A hybrid intrusion detection system based on ABC-AFS algorithm for misuse and anomaly detection. *Computer Networks, 136*, 37-50. doi:10.1016/j.comnet.2018.02.028

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

Harp, N. L., & Barnes, B. G. (2018). Internal control weaknesses and acquisition performance. *The Accounting Review, 93*, 235-258. doi:10.2308/accr-51780

Hardicre, J. (2014). Valid informed consent in research: An introduction. *British Journal of Nursing, 23*, 564-567. doi:10.12968/bjon.2014.23.11.564

Harrell, M. (2017). Synergistic security: A work system case study of the target breach. *Journal of Cybersecurity Education, Research and Practice, 2017*(2), Article 4. Retrieved from https://www.digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=1027&context=jcerp

Harris, M. A., & Patten, K. P. (2014). Mobile device security considerations for small and medium-sized enterprise business mobility. *Information Management & Computer Security, 22*, 97-114. doi:10.1108/IMCS-03-2013-0019

Harrison, A. J., Dilla, W. N., & Mennecke, B. E. (2019). Relationships within the fraud diamond: The decision processes that influence fraudulent intentions in online consumer fraud. *Journal of Information Systems In-Press*. doi:10.2308/isys-52627

Hays, D. G., Wood, C., Dahl, H., & Kirk-Jenkins, A. (2016). Methodological rigor in Journal of Counseling & Development qualitative research articles: A 15-year review. *Journal of Counseling & Development, 94,* 172-183. doi:10.1002/jcad.12074

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

Heale, R., & Forbes, D. (2013). Understanding triangulation in research. *Evidence Based Nursing, 16*(4), 98. doi:10.1136/eb-2013-101494

Henderson, H. (2018). Difficult questions of difficult questions: the role of the researcher and transcription styles. *International Journal of Qualitative Studies in Education, 31,* 143-157. doi:10.1080/09518398.2017.1379615

Hesse-Biber, S. (2015). The problems and prospects in the teaching of mixed methods research. *International Journal of Social Research Methodology, 18,* 463-477. doi:10.1080/13645579.2015.1062622

Hintze, M. (2018). Data controllers, data processors, and the growing use of connected products in the enterprise: Managing risks, understanding benefits, and complying with the GDPR. *Journal of Internet Law, 22*(2), 17-31. doi:10.2139/ssrn.3192721

Hochbein, C., & Smeaton, K. (2018). An exploratory analysis of the prevalence of quantitative research methodologies in journal articles. *International Journal of Education Policy & Leadership, 13*(11), 1-17. doi:10:22230/ijepl.2018v13n11a765

Hou, Y., Gao, P., & Nicholson, B. (2018). Understanding organizational response to regulative pressure in information security management: The case of a Chinese hospital. *Technological Forecasting and Social Change, 126,* 64-75. doi:10.1016/j.techfore.2017.03.023

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

Iivari, N. (2018). Using member checking in interpretive research practice: A hermeneutic analysis of informants' interpretation of their organizational realities. *Information Technology & People, 31*, 111-133. doi:10.1108/ITP-2016-0168

Irvine, A., Drew, P., & Sainsbury, R. (2013). 'Am I not answering your questions properly?' Clarification, adequacy and responsiveness in semi-structured telephone and face-to-face interviews. *Qualitative Research, 13*, 87-106. doi:10.1177/1468794112439086

James, L. (2018). Making cyber-security a strategic business priority. *Network Security, 2018,* 6-8. doi:10.1016/S1353-4858(18)30042-4

Jayakar, K. (2018). Universal broadband: Option right or obligation. *Journal of Human Values, 24*(1), 11-24. doi:10.1177/0971685817733569

Jordan, F., Bernardy, A., Stroh, M., Horeis, J., & Stich, V. (2017, July). Requirements-based matching approach to configurate cyber-physical systems for SMEs. *In 2017 Portland International Conference on Management of Engineering and Technology (PICMET)* (pp. 1-7). IEEE. doi:10.23919/PICMET.2017.8125442

Kaba, A., Baumann, A., Kolotylo, C., & Akhtar-Danesh, N. (2017). A descriptive case study of the changing nature of nurses' work: The impact of managing infectious diseases requiring isolation. *American Journal of Infection Control, 45*(2), 200-2002. doi:10.1016/j.ajic.2016.06.036

Kachaner, N., King, K., & Stewart, S. (2016). Four best practices for strategic planning. *Strategy & Leadership, 44*(4), 26-31. doi:10.1108/SL-06-2016-0046

Kakucha, W., & Buya, I. (2018). Information system security mechanisms in financial management. *Journal of Information and Technology, 2*(1), 1-16. Retrieved from https://stratfordjournals.org

Karanja, E. (2017). The role of the chief information security officer in the management of IT security. *Information and Computer Security, 25*, 300-329. doi:10.1108/ics-02-2026-0013

Kaukola, J., Ruohonen, J., Tuomisto, A., Hyrynsalmi, S., & Leppänen, V. (2017). Tightroping between APT and BCI in small enterprises. *Information & Computer Security, 25*, 226-239. doi:10.1108/ICS-07-2016-0047Khan, S. N. (2014). Qualitative research method: Grounded theory. *International Journal of Business & Management, 9*, 224-233. doi:10.10.5539/ijbm.v9n11p224

Kelly, P., Fitzsimons, C., & Baker, G. (2016). Should we reframe how we think about physical security and sedentary behavior measures? Validity and reliability reconsidered. *International Journal of Behavioral Nutrition and Physical Activity, 13*(32), 1-10. doi:10.11.1186/s12966-016-0351-4

Korhonen, J. J. (2014). Big data: Big deal for organization design? *Journal of Organization Design, 3,* 31-36. doi:10.146/jod.3.1.13261

Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy, 41*, 1027-1038. doi:10.1016/j.telpol.2017.09.003

Kultys, J. (2016). Controversies about agency theory as theoretical basis for corporate governance. *Oeconomia Copernicana, 7*, 613-634. doi:10.12775/OeC.2016.034

Kure, H., Islam, S., & Razzaque, M. (2018). An integrated cyber security risk management approach for a cyber-physical system. *Applied Sciences, 8*, 872-898. doi:10.3390/app8060898

Lai, S., Li, H., Lin, H., & Wu, F. (2017). The influence of internal control weaknesses on firm performance. *Journal of Accounting and Finance, 17*(6), 82-95. Retrieved from http://www.na-businesspress.com/jafopen.html

Laureani, A., & Antony, J. (2019). Leadership and Lean Six Sigma: A systematic literature review. *Total Quality Management & Business Excellence, 30,* 53-81. doi:10.1080/14783363.2017.1288565

Lee, J., Cho, E., & Choi, H. (2016). The effect of internal control weakness on investment efficiency. *Journal of Applied Business Research, 32*, 649-662. doi:10.19030/jabr.v32i3.9648

Lee, Y. S. (2018). Government guaranteed small business loans and regional growth. *Journal of Business Venturing, 33,* 70-88. doi:10.1016/j.jbusvent.2017.11.001

Leedy, P. D., & Ormrod, J. E. (2015). *Practical research: Planning research: Planning and design* (11th ed.). New York, NY: Pearson.

Leung, L. (2015). Validity, reliability, and generalizability in qualitative research. *Journal of Family Medicine & Primary Care, 4*, 324-327. doi:10.4103/2249-4863.161306

Lewis, S. (2015). Qualitative inquiry and research design: Choosing among five approaches. *Health Promotion Practice, 16*, 473-475. doi:10.1177/1524839915580941

Liang, H. Y., Kuo, L. W., Chan, K. C., & Chen, S. H. (2018). Bank diversification, performance, and corporate governance: evidence from China. *Asia-Pacific Journal of Accounting & Economics*, 1-17. doi:10.1080/16081625.2018.1452618

Liang, X., Zhao, X., Wang, M., & Li, Z. (2018). Small and medium-sized enterprises sustainable supply chain financing decision based on triple bottom line theory. *Sustainability, 10*, 4242. doi:10.3390/su10114242

Lino, A., Rocha, A., Macedo, L., & Sizo, A. (2019). Application of clustering-based decision tree approach in SQL query error database. *Future Generation Computer Systems, 93*, 392-406. doi:10.1016/j.future.2018.10.038

Lowe, A., Norris, A. C., Farris, A. J., & Babbage, D. R. (2018). Quantifying thematic saturation in qualitative data analysis. *Field Methods, 30*, 191-207. doi:10.1177/1525822X17749386

Lloyd, J., & Hopkins, P. (2015). Using interviews to research body size. Methodological and ethical considerations. *Area, 47*, 305-310. doi:10.1111/area.12199

Lozupone, V. (2018). Analyze encryption and public key infrastructure (PKI). *International Journal of Information Management, 38*, 42-44. doi:10.1016/j.ijinfomgt.2017.08.004

Lyon, B. K., & Popov, G. (2017). Communicating & managing risk: The key result of risk assessment. *Professional Safety, 62*(11), 35-44. Retrieved from http://www.asse.org/professional-safety/

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

Marshall, C., & Rossman, G. B. (2016). *Designing qualitative research* (6th ed.). Thousand Oaks, CA: Sage.

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

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

McGarry, O. (2016). Knowing ‘how to go on’: Structuration theory as an analytical prism in studies of intercultural engagement. *Journal of Ethic & Migration Studies, 42*, 2067-2085. doi:10.1080/1369183X.2016.1148593

McIntosh, M. J., & Morse, J. M. (2015). Situating and constructing diversity in semi-structured interviews. *Global Qualitative Nursing Research, 2,* 1-2. doi:10.1177/2333393615597674

Melewar, T. C., Foroudi, P., Dinnie, K., & Nguyen, B. (2017). The role of corporate identity management in the higher education sector: an exploratory case study. *Journal of Marketing Communications,* 1-23. doi:10.1080/13527266.2017.1414073

Mesquida, A. L., & Mas, A. (2015). Implementing information security best practices on software lifecycle processes: The ISO/IEC 15504 security extension. *Computers & Security, 48,* 19-34. doi:10.1016/j.cose.2014.09.003

Micheli, P., & Mura, M. (2017). Executing strategy through comprehensive performance measurement systems. *International Journal of Operations & Production Management, 37*, 423-443. doi:10.1108/IJOPM-08-2015-0472

Mijnhardt, F., Baars, T., & Spruit, M. (2016). Organizational characteristics influencing SME information security maturity. *Journal of Computer Information Systems, 56*, 106-115. doi:10.1080/08874417.2016.1117369

Mitchell, A. Madill, J., & Chreim, S. (2015). Marketing and social enterprises: Implications for social marketing. *Journal of Social Marketing, 5,* 285-306. doi:10.1108/JSOCM-09-2014-0068

Mithas, S., Kude, T., & Whitaker, J. (2018). Artificial intelligence and IT professionals. *IT Professional, 20*, 6-13. doi:10.1109/MITP.2018.053891331

Moira, M., & Brid, D. (2017). Doing a thematic analysis: A practical, step-by-step guide for learning and teaching scholars. *All Ireland Journal of Teaching & Learning in Higher Education, 8*(335), 1-14. Retrieved from http://ojs.aishe.org/index.php/aishe-j/article/view/335

Moon, K., Brewer, T. D., Januchowski-Hartley, S. R., Adams, V. M., & Blackman, D. A. (2016). A guideline to improve qualitative social science in ecology and conservation journals. *Ecology and Society, 21*(3), 1-20. doi:10.5751/ES-08663-210317

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

Moussa, M. (2015). Monitoring employee behavior through the use of technology and issues of employee privacy in America. *Sage Open, 5*(2), 1-13. doi:10.1177/2158244015580168

Moustakas, C. E. (1994). *Phenomenological research methods.* Thousand Oaks, CA: Sage.

Mrabet, Z. E., Kaabouch, N., Ghazi, H. E., & Ghazi, H. E. (2018). Cyber-security in smart grid: Survey and challenges. *Computers & Electrical Engineering, 67,* 469-482. doi:10.1016/j.compeleceng.2018.01.015

Muller, R. (2009). *Project governance*. London: Routledge Publications Inc.

Mutnuru, S. (2016). The role of internal controls on employees' engagement in small organizations. *Journal of Business Studies Quarterly*, *7*(4), 102-114. Retrieved from http://jbsq.org

Nadal, K. L., Davidoff, K. C., Davis, L. S., Wong, Y., Marshall, D., & McKenzie, V. (2015). A qualitative approach to intersectional microaggessions: Understanding influences of race, ethnicity, gender, sexuality, and religion. *Qualitative Psychology, 2*, 147-163. doi:10.1037/qup0000026

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity, version 1.1*. Gaithersburg, MD. doi:10.6028/NIST.CSWP.04162018

Newington, L., & Metcalfe, A. (2014). Factors influencing recruitment to research: Qualitative study of the experiences and perceptions of research teams. *BMC Medical Research Methodology, 14,* 1-20. doi:10.1186/1471-2288-14-10

Niedbalski, J., & Ślęzak, I. (2016). Computer analysis of qualitative data in literature and research performed by polish sociologists. *Forum: Qualitative Social Research, 17*(3), 1-22. doi:10.17169/fqs-17.3.2477

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

Nofal, M. I. M., & Yusof, Z. M. (2016). Conceptual model of enterprise resource planning and business intelligence systems usage. *International Journal of Business Information Systems, 21*, 178-194. doi:10.1504/IJBIS.2016.074260

Northrup, J. C., & Shumway, S. (2014). Gamer widow: A phenomenological study of spouses of online video game addicts. *American Journal of Family Therapy, 42*, 269-281. doi:10.1080/01926187.2013.847705

Omar, M. B., & Rahman, A. B. A. (2019). Corporate governance disclosure from agency theory perspective: A conceptual model for Saudi listed companies. *International Journey of Academic Research in Business and Social Sciences, 9*, 518-530. doi:10.6007/IJARBSS/v9-i5/5901

O'Neal, S. (2016). The personal-data tsunami and the future of marketing. *Journal of Advertising Research, 56*, 136-141. doi:10.2501/JAR-2016-027

Onwujekwe, G., Thomas, M., & Osei-Bryson, K. M. (2019, April). Using robust data governance to mitigate the impact of cybercrime. In *Proceedings of the 2019 3rd*

International Conference on Information System and Data Mining (pp. 70-79). doi:10.1145/3325917.3325923

Osanloo, A., & Grant, C. (2016). Understanding, selecting, and integrating a theoretical framework in dissertation research: Creating the blueprint for your “house”. *Administrative issues journal: connecting education, practice, and research, 4*(2), 12-26. doi:10.5929/2014.4.2.9

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

Panda, R., & Kapoor, D. (2017). Relationship between information systems integration, innovation and consumer-based commitment practices for knowledge sharing in creating power brands. *Trziste= Market*, *29*, 59-74. doi:10.22598/mt/2017.29.1.59

Park, J., & Campbell, J. M. (2018). US small business’s philanthropic contribution to local community: Stakeholder salience and social identity perspectives. *Journal of Nonprofit & Public Sector Marketing*, *30*, 317-341. doi:10.1080/10495142.2018.1452823

Park, J., & Park, M. (2016). Qualitative versus quantitative research methods: Discovery or justification? *Journal of Marketing Thought*, *3*, 1-7. doi:10.15577/jmt.2016.03.01.1

Park, K., Woo, S., Moon, D., & Choi, H. (2018). Secure cyber deception architecture and decoy injection to mitigate the inside threat. *Symmetry, 10*(1), 14. doi:10.3390/sym10010014

Patton, M. (2002). *Qualitative research and evaluation methods.* London, England: Sage.

Paulsen, C. (2016). Cybersecuring small business. *Computer, 49*(8), 92-97. doi:10.1109/MC.2016.223

Pearce, P., Ensafi, R., Li, F., Feamster, N., & Paxson, V. (2018). Toward continual measurement of global network-level censorship. *IEEE Security & Privacy, 16*(1), 24-33. doi:10.1109/MSP.2018.1331018

Pearson, M. L., Albon, S. P., & Hubball, H. (2015). Case study methodology: Flexibility, rigour, and ethical considerations for the scholarship of teaching and learning. *Canadian Journal for the Scholarship of Teaching and Learning, 6*(3), 12. doi:10.5206/cjsotl-rcacea.2015.3.12

Peltier-Rivest, D. (2018). A model for preventing corruption. *Journal of Financial Crime, 25*, 545-561. doi:10.1108/JFC-11-2014-0048

Penuel, W. R., Farrell, C. C., Allen, A. R., Toyama, Y., & Coburn, C. E. (2018). What research district leaders find useful. *Educational Policy, 32*, 540-568. doi:10.1177/0895904816673580

Piggin, R. (2016). Cyber security trends: What should keep CEOs awake at night. *International Journal of Critical Infrastructure Protection, 13,* 36-38. doi:10.1016/j.ijcip.2016.04.001

Pinfield, S., Cox, A. M., & Smith, J. (2014). Research data management and libraries: Relationships, activities, drivers, and influences. *Plos ONE, 9*, 1-28. doi:10.1371/journal.pone.0114734

Plachkinova, M., & Maurer, C. (2018). Teaching case security breach at Target. *Journal of Information Systems Education, 29*, 11-19. Retrieved from http://www.jise.appstate.edu

Prajogo, D., Toy, J., Bhattacharya, A., Oke, A., & Cheng, T. C. E. (2018). The relationships between information management, process management and operational performance: Internal and external contexts. *International Journal of Production Economics, 199*, 95-103. doi:10.1016/j.ijpe.2018.02.019

Prokhorova, V. V., & Zakharova, E. N. (2016). Peculiarities of corporate governance methodology. *Journal of Internet Banking and Commerce, 21*(1), 1-15. Retrieved from http://www.arraydev.com/commerce/jibc/

Qu, T., Thurer, M., Wang, J., Wang, Z., Fu, H., Li, C., & Huang, G. Q. (2017). System dynamics analysis for an Internet-of-Things-enabled production logistics system. *International Journal of Production Research*, *55*, 2622-2649. doi:10.1080/00207543.2016.1173738

Radchenko, A., Kolodeznaia, G., & Karpovich, I. (2019). Solving the problem of income loss in the networks of the transport telecommunications operator when providing the VPN service. In *International Scientific Siberian Transport Forum* (pp. 233-244). doi:10.1007/978-3-030-37916-2_24

Rae, K., Sands, J., & Subramaniam, N. (2017). Associations among the five components within COSO internal control-integrated framework as the underpinning of quality corporate governance. *Australasian Accounting Business & Finance Journal*, *11*(1), 28-54. doi:10.14453/aabfj.v11i1.4

Raiborn, C., Butler, J. B., Martin, K., & Pizzini, M. (2017). The internal audit function: A prerequisite for good governance. *Journal of Corporate Accounting & Finance, 28*(2), 10-21. doi:10.1002/jcaf.22246

Reinecke, J., Arnold, D. G., & Palazzo, G. (2016). Qualitative methods in business ethics, corporate responsibility, and sustainability research. *Business Ethics Quarterly, 26*, xiii-xxii. doi:10.1017/beq.2016.67

Rendon, J. M., & Rendon, R. G. (2016). Procurement fraud in the US Department of Defense. *Managerial Auditing Journal, 31*, 748-767. doi:10.11108/maj-11-2015-1267

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

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

Rija, M., & Rubino, F. E. (2018). The internal control systems integrated into the various profiles of governance, audit, risk, and compliance. *International Journal of Business and Management, 13,* 21-36. doi.10.5539/ijbm.v13n5p21

Rose, C., & Flynn, C. (2018). Animating social work research findings: A case study of research dissemination to benefit marginalized young people. *Visual Communication, 17*(1), 25-26. doi:10.1177/1470357217727677

Rosenthal, M. (2016). Methodology matters: Qualitative research methods: Why, when, and how to conduct interviews and focus groups in pharmacy research. *In currents in pharmacy teaching and learning, 8*, 509-516. doi:10.1016/j.cptl.2016.03.021

Rothrock, R., Kaplan, J., & van Der Oord, F. (2018). The board's role in managing cybersecurity risks. *MIT Sloan Management Review, 59*, 12-15. Retrieved from https://sloanreview.mit.edu/article/the-boards-role-in-managing-cybersecurity-risks/

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

Rousseeau, D., Billingham, J., Wilby, J., & Blachfellner, S. (2016). In search of general systems theory. *Systema: Connecting Matter, Life, Culture and Technology*, *4*(1) 76-99. doi:10.3390/IS4SI-2017-03957

Rubin, H. J., & Rubin, I. S. (2012). *Qualitative interviewing: The art of hearing data* (3rd ed.). Thousand Oaks, CA: Sage Publications Inc.

Ruggiero, P., & Cupertino, S. (2018). CSR strategic approach, financial resources, and corporate social performance: The mediating effect of innovation. *Sustainability, 10*, 3611. doi:10.3390/su10103611

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

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

Sargeant, J. (2012). Qualitative research part II: Participants, analysis, and quality assurance. *Journal of Graduate Medical Education, 4*(1), 1-3. doi:10.4300/JGME-D-11-00307.1

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

Saunders, B., Kitzinger, J., & Kitzinger, C. (2015). Anonymising interview data: Challenges and compromise in practice. *Qualitative Research*, *15*, 616-632. doi:10.1177/1468794114550439

Schneider, F. B. (2018). Impediments with policy intervention to foster cybersecurity. *Communications of the ACM, 61*, 36-38. doi:10.1145/3180493

Schoemaker, P. J., Heaton, S., & Teece, D. (2018). Innovation, dynamic capabilities, and leadership. *California Management Review, 61*(1), 15-42. doi:10.1177/0008125618790246

Seibert, S. E., Sargent, L. D., Kraimer, M. L., & Kiazad, K. (2017). Linking developmental experiences to leader effectiveness and promotability: The mediating role of leadership self-efficacy and mentor network. *Personnel Psychology, 70*, 357-397. doi:10.111/peps.12145

Selznick, L. F., & Lamacchia, C. (2018). Cybersecurity liability: How technically savvy can we expect small business owners to be? *Journal of Business & Technology Law, 13*, 217-253. Retrieved from http://www.law.unmaryland.edu/journal/jbtl/

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

Sepulveda, D. A. (2017). The role of leadership in internet governance. *Fletcher Forum of World Affairs, 41*, 129-139. Retrieved from http://www.fletcherforum.org/

Shabri, S. M., Saad, R. A. J., & Bakar, A. A. (2016). The effects of internal control systems on cooperative's profitability: A case of Koperasi ABC Berhad. *International Review of Management and Marketing, 6*, 240-245. Retrieved from http://www.econjournals.com

Shao, Z. (2019). Interaction effect of strategic leadership behaviors and organizational culture on IS-business strategic alignment and enterprise systems assimilation. *International Journal of Information Management, 44*, 96-108. doi:10.1016/j.ijinfomgt.2018.09.010

Shao, Z., Feng, Y., & Hu, Q. (2016). Effectiveness of top management support in enterprise systems success: a contingency perspective of fit between leadership style and system life-cycle. *European Journal of Information Systems, 25*, 131-153. doi:10.1057/ejis.2015.6

Shedden, P., Ahmad, A., Smith, W., Tscherning, H., & Scheepers, R. (2016). Asset identification in information security risk assessment: A business practice approach. *Communications of the Association for Information Systems, 39,* 297-320. doi:10.17705/1CAIS.03915

Sherif, K., Pitre, R., & Kamara, M. (2016). Why do information system controls fail to prevent unethical behavior? *VINE Journal of Information and Knowledge Management Systems, 46*, 251-266. doi:10.1108/vjikms-04-2015-0028

Shetty, S., McShane, M., Zhang, L., Kesan, J. P., Kamhoua, C. A., Kwiat, K., & Njilla, L. L. (2018). Reducing informational disadvantages to improve cyber risk management. *The Geneva Papers on Risk and Insurance-Issues and Practice, 43*, 224-238. doi:10.1057/s41288-018-0078-3

Shi, W., Connelly, B. L., & Hoskisson, R. E. (2017). External corporate governance and financial fraud: Cognitive evaluation theory insights on agency theory prescriptions. *Strategic Management Journal, 38*, 1268-1286. doi:10.1002/smj.2560

Siegner, M., Hagerman, S., & Kozak, R. (2018). Going deeper with documents: A systematic review of the application of texts in social research on forests. *Forest Policy & Economics, 92*, 128-135. doi:10.1016/j.forpol.2018.05.001

Silva Martins, O., & Ventura Júnior, R, (2020). The influence of corporate governance on the mitigation of fraudulent financial reporting. *Revista Brasileira de Gestão de Negócios, 22,* 65-84. doi:10.7819/rbgn.v22i1.4039

Silvia, M. (2015). Economic globalization: From microeconomic foundation to national determinants. *Procedia Economics and Finance, 27*, 731-735. doi:10.1016/S2212-5671(15)01055-2

Škrjanc, I., Ozawa, S., Ban, T., & Dovžan, D. (2018). Large-scale cyber attacks monitoring using evolving cauchy possibilistic clustering. *Applied Soft Computing, 62,* 592-601. doi:10.1016/j.asoc.2017.11.008

Smith, E., Corzine, S., Racey, D., Dunne, P., Hassett, C., & Weiss, J. (2016). Going beyond cybersecurity compliance: What power and utility companies really need to consider. *IEEE Power and Energy Magazine, 14*(5), 48-56. doi:10.1109/MPE.2016.2573898

Smith, K. H., Mendez Mediavilla., F. A., & White, G. L. (2018). The impact of online training on Facebook privacy. *Journal of Computer Information Systems, 58*, 244-252. doi:10.1080/08874417.2016.1233001

Sun, J., Wu, S., & Yang, K. (2018). An ecosystemic framework for business sustainability. *Business Horizons, 61,* 59-72. doi:10.1016/j.bushor.2017.09.006

Symantec Corporation. (2017). *Internet security threat report (ISTR) 2017* (Volume 22). Mountain View, CA: Author. Retrieved from https://www.symantec.com

Taillat, S. (2019). Disrupt and restraint: The evolution of cyber conflict and the implications for collective security. *Contemporary Security Policy, 40*, 368-381. doi:10.1080/13523260.2019.1581458

Tracy, S. (2010). Qualitative quality: Eight “big-tent” criteria for excellent qualitative research. *Qualitative Inquiry, 16,* 837-851. doi.10.1177/1077800410383121

Turner, J. R., Baker, R., & Kellner, F. (2018). Theoretical literature review: Tracing the life cycle of a theory and its verified and falsified statements. *Human Resource Development Review, 17*, 34-61. doi:10:1177/1534484317749680

Turner, S., & Endres, A. (2017). Strategies for enhancing small business owners' success rates. *International Journal of Applied Management and Technology, 16*, 34-39. doi:10.5590/IJAMT.2017.16.1.03

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

U.S. Small Business Association. (2019a). *Dynamic small business search.* Retrieved from SBA website: http://dsbs.sba.gov/dsbs/search/dsp_dsbs.cfm

U.S. Small Business Association (SBA. (2019b). *Resource guide for small businesses: U.S. small business administration, Alabama.* Retrieved from SBA website: https://www.sba.gov/offices/district/al/birmingham

U.S. Small Business Association (SBA). (2019c). *Summary of size standards by industry sector*. Retrieved from SBA website: https://www.sba.gov

U.S. Small Business Association (SBA). (2019d). *Table of Small Business Size Standards: Matched to North American Industry Classification System Codes.* Retrieved from SBA website: https://www.sba.gov/sites/default/files/files/Size_Standards_Table.pdf

Usman, M., Jan, M. A., He, X., & Chen, J. (2019). A survey on representation learning efforts in cybersecurity domain. *ACM Computing Surveys (CSUR), 52*, 111-112. doi:10.1145/3331174

Valipoor, S., & Pati, D. (2016). Making your instruments work for you. *HERD: Health Environments Research & Design Journal, 9,* 236-243. doi.10.1177/1937586715601423

Van Assche, K., Verschraegen, G., Valentinov, V., & Gruezmacher, M. (2019). The social, the ecological, and the adaptive. von Bertalanffy's general systems theory and the adaptive governance of social-ecological systems. *Systems Research and Behavioral Science, 36*, 308-321. doi:10.1002/sres.2587

Van Looy, A., & Van den Bergh, J. (2018). The effect of organization size and sector on adopting business process management. *Business & Information Systems Engineering, 60,* 479-491. doi:10.1007/s12599-017-0491-3

Vitel, P., & Bliddal, H. (2015). French cyber security and defense: An overview. *Information & Security: An International Journal, 32*, 29-41. doi:10.11610/isij.3209

Vlad, K. (2017). The Internet of things and new business opportunities. *Business Horizons, 60,* 831-841. doi:10.1016/j.bushor.2017.07.009

Voinea, C. (2018). Designing for conviviality. *Technology in Society, 52*, 70-78. doi:10.1016/j.techsoc.2017.07.002

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

von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security, 38*, 97-102. doi:10.1016/j.cose.2013.04.004

Voris, J., Song, Y., Ben Salem, M., & Stolfo, S. (2016, December). You are what you use: an initial study of authenticating mobile users via application usage. In *Proceedings of the 8th EAI International Conference on Mobile Computing, Applications and Services* (pp. 51-61). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering). doi:10.4108/eai.30-11-2016.2267094

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*, 23-30. Retrieved from http://jwpress.com/

Watts, L. L., Todd, E. M., Mulhearn, T. J., Medeiros, K. E., Mumford, M. D. & Connelly, S. (2016). Qualitative evaluation methods in ethics education: A systematic review and analysis of best practices. *Accountability in Research, 24*, 225-242. doi:10.1080/08989621.2016.1274975

Weishäupl, E., Yasasin, E., & Schryen, G. (2018). Information security investments: An 161 exploratory multiple case study on decision-making, evaluation, and learning. *Computers & Security, 77*, 807-823. doi:10.1016/j.cose.2018.02.001

Welch, D., Grossaint, K., Reid, K., & Walker, C. (2014). Strengths-based leadership development: Insights from expert coaches. *Consulting Psychology Journal: Practice & Research, 66*, 20-37. doi:10.1037/cpb0000002

Williams, M. L., Levi, M., Burnap, P., & Gundur, R. V. (2019). Under the corporate radar: Examining insider business cybercrime victimization through an application of routine activities theory. *Deviant Behavior, 40*, 1119-1131. doi:10.1080/01639625.2018.1461786

Wong, A., Holmes, S., & Schaper, M. T. (2018). How do small business owners actually make their financial decisions? Understanding SME financial behavior using a case-based approach. *Small Enterprise Research, 25*, 36-51. doi:10.1080/13215906.2018.1428909

Xu, M. A., & Storr, G. B. (2012). Learning the concept of researcher as instrument in qualitative research. *Qualitative Report*, 17, 1-17. Retrieved from http://tqr.nova.edu

Yazan, B. (2015). Three approaches to case study methods in education: Yin, Merriam, and Stake. *Qualitative Report, 20*, 134-152. Retrieved from http://www.nova.edu/tqr/

Yi, H., & Scholz, J. T. (2016). Policy networks in complex governance subsystems: observing and comparing hyperlink, media, and partnership networks. *Policy Studies Journal*, *44*, 248-279. doi:10.1111/psj.12141

Yilmaz, K. (2013). Comparison of quantitative and qualitative research traditions: Epistemological, theoretical, and methodological differences. *European Journal of Education, 48*, 311-325. doi:10.1111/ejed.12014

Yin, R. K. (2012). *Application of case study research*. Thousand Oaks, CA: Sage Publications, Inc.

Yin, R. K. (2017). *Case study research and applications: Design and methods* (6th ed.). Thousand Oaks, CA: Sage Publications, Inc.

Yoo, Y. S., Park, H. G., Back, S. H., & Hong, S. C. (2017). A study on procurement audit integration real time monitoring system using process mining under big data environment. *Journal of Internet Computing and Services, 18*(3), 71-83. doi:10.7472/jksii.2017.18.3.71

Zager, L., Malis, S. S., & Novak, A. (2016). The role and responsibility of auditors in prevention and detection of fraudulent financial reporting. *Procedia Economics and Finance, 39*, 693-700. doi:10.1016/S2212-5671(16)30291-X

Zainal, Z. (2017). Case study as a research method. *Jurnal Kemanusiaan, 5*(1), 1-6. Retrieved from http://www.jurnal-kemanusiaan.utm.my/index.php/kemanusiaan/article/viewFile/165/158

Zhang, W., Wang, Z., Liu, Y., Ding, D., & Alsaadi, F. E. (2018). Sampled-data consensus of nonlinear multiagent systems subject to cyber attacks. *International Journal of Robust and Nonlinear Control, 28*(1), 53-67. doi:10-1002/mc.3855

Zubiaga, A., Procter, R., & Maple, C. (2018). A longitudinal analysis of the public perception of the opportunities and challenges of the Internet of Things. *PLoS ONE, 13*(12), 1-18. doi:10.1371/journal.pone.0209472

Zuckweiler, K. M., Rosacker, K. M. & Hayes, S. K. (2016). Business students' perceptions of corporate governance best practices. *Corporate Governance: The International Journal of Business in Society, 16,* 361-376. doi:10.1108/cg-08-2015-0117

Appendix A: Interview Protocol

Project: Walden University Doctorate of Business Administration (DBA) Study

Type of Interview:____

Date:____

Place:____

Interviewer:____

Interviewee:____

Position Title of Interviewee:____

[Describe the project; explain to the interviewee about the (a) purpose of the study, (b) multiple sources of data collection, (c) data confidentiality, and (d) completion of the interview in less than one hour.] [Provide the interviewee with contact information.] [Request the SME owner provide copies of any additional relevant company documentation he/she would like to share.] [Remind the interviewee of the consent form to participate in the study and to audio record the interview (provide copy if required).] [Turn on the digital audio recorder and test device for functionality.]

Interview Questions:

1. What business strategies do you use to reduce cyberattacks to remain profitable?
2. How did you develop successful strategies to reduce cyberattacks to remain profitable?
3. What strategies were not successful in reducing cyberattacks to remain profitable?
4. What, if any, key barriers existed to implementing strategies to reduce cyberattacks to remain profitable?

5. How did you address these key barriers to implementing strategies to reduce cyberattacks to remain profitable?
6. What additional information can you share regarding strategies for reducing cyberattacks that we have not already discussed?

[Thank the interviewees for their assistance and participation in the interview. Reiterate the study’s anonymity of the respondent’s responses. Inform the interviewee you will provide him/her a copy of the transcription file for review, approval, and return.]

Appendix B: Invitational Email for Participants

Greetings:

My name is Ira J. Phillips, Jr., and I am a doctoral candidate at Walden University. I am conducting a research study focused on small business owners who have successful strategies to reduce cyberattacks to remain profitable in central Alabama. The study will occur in the form of interviews that I will facilitate. The confidentiality of the Participant will be protected during data collection and reporting results.

This e-mail correspondence is a request for participants for this voluntary study to begin this collaborative research on successful business strategies for countering cyberattacks to remain profitable. If you are interested in participating in the study, please send me an e-mail directly at [redacted] and I will provide you with the necessary paperwork for informed consent for your review and completion.

Please e-mail me at the following e-mail address, if you require additional information before making your decision.

As a reminder, participation is voluntarily and confidential.

Thank you for your time and consideration in contributing to this study.

Sincerely,

Ira J. Phillips, Jr., MHS

[e-mail address redacted]