2020

Strategies to Reduce Small Business Data Security Breaches

Sikini Knight

Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Sikini Knight

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. Diane Dusick, Committee Chairperson, Doctor of Business Administration Faculty

Dr. Judith Blando, Committee Member, Doctor of Business Administration Faculty

Dr. Jorge Gaytan, University Reviewer, Doctor of Business Administration Faculty

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

Walden University
2020

Abstract

Strategies to Reduce Small Business Data Security Breaches

by

Sikini Knight

MS, William Carey University, 2008

BS, University of Southern Mississippi, 2004

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

April 2020

Abstract

Organizations affected by data security breaches may experience reputational damage and remediation costs. Understanding the data security strategies needed to protect small businesses is vital to safeguard company data and protect consumers' personal information. Grounded in systems theory, the purpose of this qualitative multiple case study was to explore the strategies small business owners use to reduce data security breaches. The participants were 4 small business owners located in the southern region of the United States: 2 franchise small business owners and 2 nonfranchise small business owners. Data were collected from semistructured interviews and organizational documents. Yin's 5-step data analysis was used to analyze the data. Two themes emerged: information assurance and third-party dependencies. A key recommendation includes small business owners implementing a contingency plan to manage a data security breach. The implications of positive social change include the potential for small business owners to develop data security strategies to protect their organizations from experiencing a data breach. Protection from data breaches can, in turn, rebuild trust with small business owners and increase spending, increasing the local community's tax base that may be used to improve social services in the local community.

Strategies to Reduce Small Business Data Security Breaches

By

Sikini Knight

MS, William Carey University, 2008

BS, University of Southern Mississippi, 2004

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

April 2020

Dedication

I want to dedicate this work to my son (Scottie Moody Jr.). You were the peace in my storm. Some people said that my progress in this program would stop after I got pregnant. It was quite the opposite. Having you gave me motivation. I hope that I have made you proud.

Acknowledgments

I want to thank every individual who encouraged me to complete this journey. Mom and dad, I can never say thank you enough for being the best parents in the world and supporting my dreams. Many thanks to Dr. Dusick, Dr. Blando, and Dr. Gaytan for serving on my committee and pushing me to places that I did not think my mind could reach. You all were God sent and truly instrumental in my growth during this process. I would also like to thank all of my friends and family and especially my parents, who stuck by me every step of the way.

Folake Ige, you were one of my biggest inspirations. You were there through all of the tears and long nights. Thank you, cousin, for believing in me and encouraging me never to quit. Thank you for everything. Hope Stallworth, we did it! I could not have picked a better friend to take on this journey.

To my nieces, nephews, cousins, siblings, and most importantly, my son always believe in the impossible. You can accomplish all of your goals. When I started this journey (college), I had a counselor who discouraged me from entering the field of technology. She said to me that those people are “smart.” I was truly on fire after that comment, and I continued my education to prove to myself and others that anything is possible. Never let anyone stop you from striving for the best.

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

In 2017, hackers compromised approximately 7,125,940 records daily (Sivagnanam, 2018). Researchers have offered little information on the strategies needed to protect organizations from data security breaches (Horne, Maynard, & Ahmad, 2017). Data security breaches have negative influences on an organization's performance (Zafar, Ko, & Osei-Bryson, 2016). Identifying strategies to reduce data security breaches could lay the foundation for improved data security protection.

Background of the Problem

Business leaders are using data communication and web-based technology to manage organizational activities (Safa & Solms, 2016). Technology leaders reported an increase in data security threats in organizations using information-based technology (Horne et al., 2017). Hackers have used data from information-based technology to access financial and private data (Horne et al., 2017). Hackers are people or entities illegally accessing unauthorized information. Illegally obtaining information violates data security measures information security officers create, potentially costing businesses billions of dollars (Samtani, Chinn, Chen, & Nunamaker, 2017).

The Identity Theft Resource Center reported that nearly 381 data security breaches resulted in the theft of 10 million private records (Chakraborty, Lee, Bagchi-Sen, Upadhyaya, & Raghav Rao, 2016). Small and medium enterprises (SMEs) experienced approximately 72% of data security breaches (Fielder, Panaousis, Malacaria, Hankin, & Smeraldi, 2016). Hackers target small businesses because of their size (Rosenstein, 2017). Small business owners may experience bankruptcy if they encounter a security breach (Rosenstein, 2017). Some retailers have lost as much as $291 million on one breach related activity (Rosenstein, 2017). Data security breaches cause information security officers to look for ways to prevent data security breaches (Gordon, Loeb, Lucyshyn, & Zhou, 2018). Providing small business owners with the strategies needed to reduce data security breaches could reduce data security breaches.

Problem Statement

Organizations affected by data security breaches may experience reputational damage and remediation costs (Gwebu, Wang, & Wang, 2018). Tadesse and Murthy (2018) reported that small business owners experience 71% of all data security breaches. Seventy-nine percent of small business owners have not created a plan to respond to a cyber-attack (Rohn, Sabari, & Leshem, 2016). The general business problem is the inability of some small business owners to manage data security performance, resulting in increased data security breaches and loss of business profitability. The specific business problem is that some small business owners lack strategies to reduce data security breaches.

Purpose Statement

The purpose of this qualitative multiple case study was to explore strategies small business owners use to reduce data security breaches. The targeted population consisted of four small business owners with successful experience in reducing data security breaches. The geographical location of the study was in the southern region of the United States. The study may contribute to positive social change by rebuilding the relationships between business leaders and consumers. Rebuilding relationships between business leaders and consumers could result in increased spending to support local communities and improve the financial health of the local economy (Nguyen, Newby, & Macaulay, 2015).

Nature of the Study

When selecting a research method, a researcher may choose the qualitative, quantitative, or mixed research method. I selected the qualitative method to capture the human experience. Qualitative researchers use open-ended questions to capture the human experience and explore a phenomenon (Athukorala, Głowacka, Jacucci, Oulasvirta, & Vreeken, 2016; Yin, 2018). On the contrary, quantitative researchers define and quantify a problem by using numerical results (Yin, 2018). The mixed methods approach requires the researcher to spend more time analyzing both qualitative and quantitative research (Yin, 2018). To explore the various strategies some small business owners use to reduce data security breaches, I did not analyze quantitative or mixed method data. I elected to analyze rich textural data to explore specific strategies.

I considered three research designs to explore the study: (a) case study, (b) narrative, and (c) phenomenological. I chose a multiple case study design. A multiple case study was an appropriate design when the researcher is asking *what*, *why*, and *how* questions about a phenomenon under investigation in its natural context (Yin, 2018). Researchers conduct case studies to explore a phenomenon using multiple data sources. Unlike a case study, narrative design requires extensive information (Yin, 2018). Researchers may experience issues encountered during the data collection process and analysis phase because the narrative has to determine who owns the story, who will tell the story, and whose version will convince the audience of the story (Graci & Fivush, 2017). Researchers use a phenomenological design to interpret the participants' lived experiences of a phenomenon by focusing on the individual and not the factors that influence a phenomenon (Cibangu & Hepworth, 2016; Creswell, & Poth, 2018). Neither the narrative nor phenomenological design was appropriate for this study because I did not seek to explore the stories or lived experiences of the participants.

Research Question

The overarching research question for the study was as follows: What strategies do small business owners use to reduce data security breaches?

Interview Questions

1. What strategies did you use to reduce security breaches in your organization?
2. How is data security performance measured in your organization?
3. How would your organization address internal or external data security breaches?
4. How are you training your employees to protect your organization's data from a data security breach?
5. How have your existing policies and procedures protected your organization's data security environment against intrusions from outsiders and insiders (intentional or unintentional)?
6. How does your organization back up sensitive data?
7. What else can you add to help other business leaders reduce data security breaches?

Conceptual Framework

Bertalanffy (1968) developed systems theory in the 1950s to describe the interrelated parts of a complete system, as opposed to defining the system as individual parts. Systems theory applies to fields, such as industrial engineering, science, humanities, and technology (Adams, Hester, Bradley, Meyers, & Keating, 2014; Bertalanffy, 1968). The tenets of systems theory are (a) input, (b) output, (c) feedback, and (d) environment (Seiler & Kowalsky, 2011).

Systems theory was appropriate for the study because the framework was a holistic approach to viewing the entire data security system as opposed to viewing the parts as separate entities. Viewing the system comprehensively reduces the complexity of trying to understand multiple parts of a system (Arnold & Wade, 2015). Systems theory is a set of collective interactions used to improve an individual's ability to recognize and understand systems while predicting the behaviors and modifying the systems to deliver the desired outcomes (Arnold & Wade, 2015). Applying systems theory to the study promoted exploring strategies to influence the interconnections, feedback, and different behaviors of the system. Identifying interconnections and feedback in a system contribute to gaining insight into the structure of the system (Arnold & Wade, 2015).

Operational Definitions

Alphanumeric passwords: Alphanumeric passwords are a combination of letters and numbers used in a system to authenticate a user (Catuogno & Galdi, 2014).

Cybersecurity: Cybersecurity is an illegal act committed with or against an individual or organization’s computer or network (U.S. Department of Homeland Security, 2019a).

Data security breach: Data security breach is an illegal intrusion or access to information that may or may not affect an individual or organization (Jackson, 2018).

Hackers: Hackers are intelligent individuals who manipulate computer software and network systems beyond the original intent (Dadkhah, Lagzian, & Borchardt, 2018).

Iris-scans: Iris-scans are biometric identification method that uses the iris of an individual’s eye to authenticate the user (Ribeiro, Uhl, & Alonso-Fernandez, 2019).

Pin-based authentication: Organizational leaders use pin-based authentication to allow users to input a numeric identification code (Saulynas, Lechner, & Kuber, 2018).

PAKE: Password-authenticated key exchange (PAKE) is a security method that allows a user and the server to verify the authentication through one of the parties’ knowledge of the password (Soni, Pachouri, & Jain, 2018).

Assumptions, Limitations, and Delimitations

Assumptions

Assumptions are ideas appearing to be true without validation (Schoenung & Dikova, 2016). Four assumptions were appropriate for this study. A qualitative case study was applicable to address the research problem. A purposive sample size of four participants appropriately represented the population of small businesses in the southern United States. I assumed that participants would be honest and forthcoming when responding to the interview process. Finally, I assumed that small business owners were willing to share their data security strategies.

Limitations

Limitations are potential weaknesses discovered by the researcher (Marshall & Rossman, 2016). Time constraints could limit extensive research. To alleviate time constraints, I provided the participants with the interview questions after determining if the participants met the eligibility criteria. I provided the participants with the interview questions no less than one week before the interview to help expedite the data collection process. Participants could have limited the results if they were not honest and forthcoming. I experienced limitations while finding potential participants. Participants appeared uncomfortable discussing data security with me over the phone. I also failed to receive any feedback from participants by mail or email. To mitigate the trust issues with gaining access to the participants, I elected to search for participants over the phone or face-to-face. Requesting participation over the phone and face-to-face increased trust with the participants.

Case study researchers may experience bias because of the personal experiences related to the study (Yin, 2018). The research validation process included member checking to reduce or mitigate research biases. Member checking is a respondent validation process that establishes credibility for the data collection results (Birt, Scott, Cavers, Campbell, & Walter, 2016). Voluntary participation could have limited the study because participants could withdraw at any time.

Delimitations

Delimitations are bounds used to narrow the scope of research (Marshall & Rossman, 2016; Yin, 2018). I selected four participants. Participants were small business owners with fewer than 1500 employees. The small business owner was in business for at least 5 years. The participants also had a strategic plan implemented to handle a data security threat. The study was bound to the location of the study. Individuals outside of the southern region of the United States were not eligible to participate. Confining the research to the southern region of the United States limited the participant pool. I used a qualitative case study design; as a result, I was unable to generalize to a larger population. To improve repeatability, I documented the entire process used to collect data.

Significance of the Study

Contribution to Business Practice

Business leaders could spend approximately $3.5 million after experiencing a data security breach (Vavilis, Petković, & Zannone, 2016). While new technology could contribute to data security issues, new and innovative technology is more likely to keep businesses innovative and efficient (Maughan, Balenson, Lindqvist, & Tudor, 2015). Business leaders need effective strategies to protect the organization's data. The findings of the study may be of value to businesses by providing small business owners with the strategies needed to reduce data security breaches.

Data are significant for business leaders to perform daily activities (Liao & Chen, 2019). Data security issues cause ineffective systems and loss of profitability

(McPherson, 2014). Implementing better data security strategies may contribute to effective business practices by reducing internal and external data security issues and improving organizational productivity and profitability.

Implications for Social Change

Individuals, organizations, and society may benefit from the results of the study by learning more about the strategies needed by small business owners to reduce data security breaches. The results may contribute to positive social change by giving business leaders the confidence and procedures necessary to protect the consumer and organizational data from criminals who intend to use the data for unlawful purposes. Protecting consumers' data from theft could rebuild trust from consumers, encourage consumers to spend more, and improve the health of the economy (Curtis, Carre, & Jones, 2018).

A Review of the Professional and Academic Literature

Data security issues have affected the security and financial growth of businesses (Elhai & Hall, 2016; Noguerol, & Branch, 2018). Small and medium enterprise (SME) business owners have dismissed the importance of data security because they did not believe they were targets of cyber attacks (Almeida, Carvalho, & Cruz, 2018). Nearly 45% of the American population has experienced a data security breach from an unsecured business (Elhai & Hall, 2016). The urgency to improve data security has increased as companies have increased their use of technology (Berry & Berry, 2018; Hess & Cottrell, 2016). Scholars have addressed data security issues by studying how to recover from a breach, types of breaches, and how technology has affected small businesses (Elhai & Hall, 2016). In this segment, I offer a comprehensive critique of the literature regarding the strategies needed by leaders of small businesses to reduce data security breaches. I identified gaps in past and present research literature to justify the significance of this study.

A literature review is a cognitive operation of carrying on research in a conventional method to increase the robustness of the research (Booth, Sutton, & Papaioannou, 2016; Machi & McEvoy, 2016). To identify literature and retrieve information on this issue, I used the following databases and search engines: (a) ABI/INFORM Complete, (b) Academic Search Complete, (c) Business Source Complete, (d) Computers and Applied Science Complete, (e) Google Scholar, and (f) Yahoo. Extensive searches returned data, security-related books, journals, websites, and government articles. I assessed relevant peer-reviewed journals to obtain source material. The literature also included articles and studies grounded in qualitative, quantitative, and mixed method research. The keywords that I used were (a) *systems theory,* (b) *data security*, (c) *information security,* (d) *data security breach,* (e) *small business data security*, (f) *cybersecurity,* and (g) *strategies for data security*. The 324 references that the study contains include 300 scholarly peer-reviewed articles representing 92% of the total, 25 nonpeer-reviewed articles representing 8%, 15 government websites representing 5%, and 10 books representing 3%. The total number of references in this study published within the 2016-2020 period are 277, which is 85% of the total number. The literature review contains 201 references, with 166 references published within the

2016-2020 period, representing 82%, and 195 from scholarly peer-reviewed sources, representing 97%.

This literature review began with an evaluation of the conceptual framework of the study, focusing on the relevance of systems theory in framing data security breaches in small business organizations. I then synthesized academic literature related to data security strategies to show the relevance and depth of existing material. The specific sections in the review are the following (a) systems theory; (b) data security in small business; (c) data security breaches; (d) implementing policies and procedures to prevent data breaches; and (e) specific strategies to protect organizational data, which includes separate discussions of passwords, employee education, data back-ups, and BYOD. The final section is a summary of the literature review and transition to the next chapter.

Systems Theory

Systems theory is the conceptual framework selected for this qualitative case study. Bertalanffy (1968) developed systems theory to understand organisms within the field of biology. Theorists later expanded the use of systems theory beyond the field of biology to study various disciplines (Hammond, 2016). Organizational leaders used systems theory to explore the behaviors of individuals in different disciplines, such as business, science, technology, biology, management, and psychology (Więcek-Janka, Mierzwiak, & Kijewska, 2016).

Bertalanffy (1968) described systems as either open or closed. In an open system, inputs interact with the environment. On the contrary, closed systems do not interact with the environment (Hughes, Newstead, Anund, Shu, & Falkmer, 2015). Business leaders prefer open systems to closed systems because open systems facilitate the operation with other organizational tasks and subsystems (Hughes et al., 2015). These subsystems are interactive with the environment (Hughes et al., 2015). For example, in small business organizations, an open system allows the small business owner to interact with vendors. Closed systems are more independent and do not require interaction from the environment to operate (Hughes et al., 2015).

The components of a system include input, output, feedback, and environment (Almaney, 1974). Input and output are transporters of information that allow system openness to measure the amount and frequency of information transported throughout the system (Almaney, 1974). Feedback is output data fed into the system as input (Williams, 2015). Managers use feedback to understand the operational effectiveness of information in a system (Williams, 2015). The application of the information in the system may have a positive or negative change within the system (Williams, 2015). Users experience negative feedback when the system interrupts the data path, whereas users experience positive feedback when the system works appropriately (Williams, 2015).

The total system bonds the external environment to create productivity within an organization (Almaney, 1974). Hence, a financial system should contain information from an external environment (Demetis, 2018). The system’s interrelated parts create customer information (Demetis, 2018). For example, a user may input their personal information on a screen. The system processes the information through the system to produce a unique banking customer with a personal bank account.

Application of systems theory in previous research. Systems theory applies to innovation (Githinji & Were, 2018). Business leaders implement innovative ideas as a way to create problem solving methods (Australian Department of Industry, Innovation, & Science, 2018). Innovation in business is implementing new ideas or changing existing processes to become more productive (Australian Department of Industry, Innovation, & Science, 2018). Some innovative ideas are related to the demands of customers and employees (Australian Department of Industry, Innovation, & Science, 2018). Customers demanding electronic processes such as electronic credit card readers have increased the innovative footprint in businesses (Clapper & Richmond, 2016). Innovative ideas can span from many ideas, including business practices, e-procurement, and organizational innovation (Githinji & Were, 2018; Rondi, De Massis, & Kotlar, 2018; Zlatanovic & Mulej, 2015).

Exploring innovative business practices, Rondi et al. (2018) used systems theory to explore the innovative potential of a family business. Rondi et al. used systems theory as a framework for understanding how the different relationships of the individuals influence the innovative practices of the business. More specifically, Rondi et al. viewed the communication of the members of the family as the collective entity that influences the entire system of family businesses.

Unlike Rondi et al. (2018), Githinji and Were (2018) utilized systems theory to understand the adoption of technological innovation such as e-procurement systems. Githinji and Were studied the challenges of implementing e-procurement in the Ministry of Transport, Infrastructure, and Housing and Urban Development in Kenya. Githinji and

Were used systems theory to view the legal framework to display how organizations interact with other outside organizations. Githinji and Were argued that implementing an e-procurement system would increase challenges such as maintaining passwords and information security. The lack of trust among the trading partners increased security threats (Githinji & Were, 2018).

Similar to Githinji and Were (2018), Zlatanovic and Mulej (2015) concentrated on innovation in companies. Zlatanovic and Mulej used systems theory to frame soft-systems approaches to the management of knowledge-cum-values as drivers of organizational innovation while Githinji and Were focused on the legal framework of how business leaders interact with external partners. Grounded from systems theory, Zlatanovic and Mulej argued that using a holistic approach is more effective as opposed to viewing organizational systems as separate entities. Despite not concentrating on the adoption of a particular technological innovation such as data security, the use of systems theory in this research study served as a justification for the relevance of framing the adoption of innovation based on the effect of implementing innovation within an organization.

In another study conducted by Abbas and Ul Hassan (2017), systems theory was one component of the framework for explaining the moderating effect of environmental turbulence on business innovation and business performance. Abbas and Ul Hassan contended that they could not isolate business innovation and performance of an organization from outside influences because firms are open systems. In this study, the outside factor of environmental turbulence served as a moderator for business innovation and business performance. Although Abbas and Ul Hassan did not specifically focus on the adoption of technology, their application of the system theory served as a justification for the effectiveness of systems theory in framing a phenomenon that involved in understanding the interrelationship of factors within an organization.

To explore technology innovation, Kretser, Ogden, Colombi, and Hartman (2016) used systems theory to study the design structure matrices to reduce enterprise information systems complexity. Organizations are large hierarchical systems that contain several interconnected subsystems (Kretser et al., 2016). As the system and the number of subsystems expanded, it became more difficult to eliminate waste and enhance organizational performance (Kretser et al., 2016). While Kretser et al. did not specifically focus on the adoption of a particular technological innovation such as data security, their application of the system theory served as a justification for the relevance of framing various phenomena from an interdependent perspective using systems theory.

In comparison to Kretser et al. (2016), Ceric (2015) applied systems theory to the field of technology to explore the functionality of a system. Both Kretser et al. and Ceric explored the systems within an organization. However, Ceric expanded the research and explored the interactions of information communication technology (ICT) and the management of systems and found that all dynamics of a system, including goals, trends, drivers, outcomes, structure, and identity, are interdependent. Each component of the system had a cause-and-effect relationship related to other elements within the system (Ceric, 2015). Experts can study a system and the interrelated elements to understand that, when one area of a system changes, other parts of the system transform based on that change (Ceric, 2015). Ceric posited that the performance of a system is contingent upon the positive interactions between the systems.

Systems theory is also applicable to the field of management. Katina (2016) used systems theory to assess the field of management by studying the relationship between systems and the environment. Katina discovered that numerous pathological conditions affect the performance in a system. Business leaders used meta-system pathology as a strategic response to handle system issues (Katina, 2016). Organizational leaders also used pathologies to describe the status of an organization’s growth and performance and the roles and responsibilities within a system (Katina, 2016). Using pathology enabled the business leaders to apply a holistic approach to understand the system (Katina, 2016).

Similar to Katina (2016), Turner and Endres (2017) examined the management of small businesses and used systems theory to explain the importance of the different interrelated components of an issue instead of concentrating on a single component. Viewing the operations of small business organizations with a holistic approach facilitated the improvement of performance (Turner & Endres, 2017). When small business owners apply systems theory within their organizations, they consider their financial actions, the different stakeholders, and social and environmental factors in conceptualizing sustainable performance (Turner & Endres, 2017). Turner and Endres also used systems theory to frame the interdependence of various activities, such as marketing and technology, in determining the success of small business organizations. Turner and Endres provided support for research regarding the appropriateness of systems theory in conceptualizing the implementation of innovation in business.

Systems theory is an appropriate framework to explore the interaction between human behavior and systems (Colangelo, 2016). Individuals are influenced by different goals based on their behavior (Ajzen, & Kruglanski, 2019). Omune and Kandiri (2018) examined hospital information systems' capability and end-user satisfaction in Kenya hospitals. Grounded on the main principle of holism in systems theory, Omune and Kandiri conceptualized the capability of a hospital for information systems based on the quality of interactions among different people within the organization. In this study, Omune and Kandiri viewed the different elements as socially based because the system's success is dependent on the contribution and interaction of the different professionals within the hospital. Specifically, the cooperation and willingness of the different social entities within an organization were necessary for the users to adopt information-based technology. Omune and Kandiri conducted a study that provided direct support for the utilization of system theory and the adoption of innovative technology.

Koral, Frank, and Miller (2018) used systems thinking to view the common problems within organizations. For instance, Koral et al. examined the development of systems thinking and the personality traits among engineers and engineering students to understand their problem-solving skills when dealing with clients. Koral et al. suggested that systems thinking enables the engineers to view the systems as a whole as opposed to viewing the interrelated parts. In addition, Koral et al. discovered that engineers with specific personality characteristics could make better decisions over time by obtaining the appropriate tools.

Unlike the work presented by Omune and Kandiri (2018) and Koral et al. (2018), Carayon et al. (2015) extended the research of human interactions and systems by applying sociotechnical systems theory to explore the critical processes involved in business organizations. For instance, Carayon et al. used sociotechnical systems theory to frame workplace safety and conceptualize the different components of safety issues in an organization. Understanding the different components allowed Carayon et al. to recognize how interrelationships operated to understand the totality of workplace dynamics. Carayon et al. combined sociotechnical systems theory to maximize the interactions between social and technical related efforts among the external environment and the complex systems utilized the leaders and employees of an organization. Complex multi-level systems contributed to workplace safety (Carayon et al., 2015). Organizational leaders should seek to increase their knowledge of the environment, organization, and system failures that contribute to workplace safety (Carayon et al., 2015). Carayon et al. used the results from the research to develop a robust solution to identify system elements and levels.

In comparison to Carayon et al. (2015), Abdullahi, Gesimba, and Gichuhi (2017) applied systems theory to frame the influence of routing and scheduling plans, logistical procedures, and customer service for courier services, as opposed to identifying system elements and levels. Leaders should view the departments and sources as a whole to determine how an organization is performing (Abdullahi et al., 2017). Abdullahi et al. found that routing and scheduling plans had a positive effect on scheduling plans, and logistical procedures had a positive effect on customer service. The different departments worked together like a system to deliver products and services to clients (Abdullahi et al., 2017). Business leaders using logistics should look for innovative ways to improve internal and external logistical processes (Abdullahi et al., 2017).

Panetto, Iung, Ivanov, Weichhart, and Wang (2019) and Haimes, Horowitz, Guo, Andrijcic, and Bogdanor (2015) focused on applying systems theory to complex technical issues, such as cyber-physical manufacturing enterprises and cloud-computing. In understanding the challenges for the cyber-physical manufacturing enterprises, Panetto et al. used the systems theory to frame their study. Panetto et al. published an article on the future manufacturing and logistics challenges facing industries from a technical perspective. The team of researchers included four technical committee members (Panetto et al., 2019). Panetto et al. studied topics that influence the manufacturing enterprise and supply chain. More specifically, the research team used systems theory to determine how systems may exist within systems but remain independent (Panetto et al., 2019). Subsystems may separate from the super systems (Panetto et al., 2019). These different elements work individually and sometimes together, to achieve a specific goal (Panetto et al., 2019). However, Panetto et al. contended that the individual elements lose their autonomy because they are part of the entire system.

Similar to Panetto et al. (2019), Haimes et al. (2015) also focused on the outcomes of systems as separate entities and as a whole, Haimes et al. used systems theory to contend that the assessment of the systemic risks in cloud-computing technology is a complex web of interconnected systems. This conceptualization of security breaches underscores the importance of viewing data security from multiple processes and components to capture the complexity of an organization (Haimes et al., 2015). Based on the different researchers having used systems theory to frame organizational processes, the central theme that emerged from the review was the need to understand how different components within an organization are interconnected and affect each other (Haimes et al., 2015; Tisdale, 2015). This perspective highlights the importance of examining multiple interrelated components of data security to acquire an accurate description of the complexity of an organization (Haimes et al., 2015).

Upholding the critical principles of systems theory, business leaders should view data security breaches systemically (Ceric, 2015; Haimes et al., 2015; Tisdale, 2015; Volkova & Kudriavtceva, 2018). Also, focusing on understanding the critical processes involved in business organizations and cybersecurity, Tisdale (2015) used systems theory to assert that an organization’s cybersecurity leaders should examine cybersecurity from a holistic view by sharing the information with the stakeholders of the organization. Also, Tisdale stated that tools and techniques are needed to organize, analyze, and share the vast amount of information needed to manage cybersecurity among the stakeholders. These interrelated components included the business, social, and information technology contexts and various organizational dynamic processes, such as operation, strategy, and management (Tisdale, 2015).

In comparison to Tisdale (2015), Dominici (2017) took a different approach to view business systems. Dominici published an article on the governance of business systems and the relevance of applying systems theory to complex systems. To stay relevant and up to date with business systems, Dominici suggested that business leaders research multiple system models and algorithms. In the findings, Dominici found that the dynamics of a system and its stability is ever changing. Similar to Tisdale, Dominici found that applying a holistic approach was appropriate to view complex systems. Dominici suggested that applying a holistic approach was essential to produce new ideas in understanding and governing complex systems (Dominici, 2017).

Applying the primary principles of systems theory to this research study may assist leaders of small business organizations in gaining the information needed to reduce their chances of experiencing a data security breach. Business leaders educating themselves on the complexity of their organization's systems are more equipped to develop successful processes and procedures (Hester, 2014). Awareness of the inputs, outputs, and the environment increases the performance of business organizations' (Hester, 2014). Using systems theory will assist business leaders in viewing the system in its entirety as opposed to viewing the system as separate entities (Hester, 2014).

Data Security in Small Business

Large corporations have high data usage (Olufemi, 2019). When the number of small businesses is combined, their aggregate data usage is comparable to large businesses (Olufemi, 2019). Businesses should implement plans to protect their data (Mubarak, 2016). Compared to big business establishments wherein leaders have the resources to address organizational data security, small businesses often do not have the same access to resources to protect their establishments from cyber threats (Berry & Berry, 2018; Hess & Cottrell, 2016; Olufemi, 2019). For instance, many small business owners do not have the resources to hire experts needed to apply the knowledge necessary to protect their data (Berry & Berry, 2018). As a result, small business owners experience challenges in managing their risk from fraudulent activities, including their ability to protect their companies from detecting fraud (Hess & Cottrell, 2016).

When business leaders decide to use technology within their organizations, they must implement security measures to prevent negative financial influence on performance. Some small business owners lack the IT techniques needed to protect their data from being compromised (Santos-Olmo, Sanchez, Caballero, Camacho, & Fernandez-Medina, 2016; Schmitz & Pape, 2020). Large corporations receive large amounts of data from small businesses with minimum security (Raghavan, Desai, & Rajkumar, 2017). Limited resources and finances create a challenge for SMEs to have a secure IT infrastructure (Coleman et al., 2016). As a result, SME leaders who fail to implement a secure IT infrastructure may experience cyber attacks.

Some small business owners fail to implement adequate cybersecurity plans because they do not believe they could become cyber targets (U.S. Department of Commerce, 2016b; U.S. Department of Homeland Security, 2018a). Because of inadequate cybersecurity plans, small business owners are often not prepared to handle a data security breach (Berry & Berry, 2018; Hess & Cottrell, 2016; U.S. Department of Commerce, 2016b). For instance, in a research study involving 400 small business firms, 27% had not implemented any cybersecurity methods (Aguilar, 2015). Approximately 60% of the participants failed to reinforce their security protocols to prevent possible security breaches (Aguilar, 2015).

Approximately 59% of SME leaders have not implemented a contingency plan to respond to a security breach (U.S. Department of Homeland Security, 2015b). Small business owners consider security plans as challenging to develop and implement (U.S. Department of Commerce, 2016b). Implementing a contingency plan could reduce the recovery time or reduce the chances of a small business owner experiencing a cyber-attack (Mubarak, 2016). Leaders should implement a contingency plan to handle sudden blackouts and natural disasters (Mubarak, 2016).

Small business owners experience more data breaches than larger corporations experience (U.S. Department of Commerce, 2016a). In 2010, the U.S. Secret Service reviewed approximately 761 data breaches; 63% of the breaches occurred at small businesses (U.S. Department of Homeland Security, 2015b). Cyber criminals target small businesses because they lack sufficient resources to contribute to cybersecurity needs (U.S. Department of Homeland Security, 2015b). In 2016, Symantec reported that leaders of small businesses encountered 43% of spear-phishing attacks, up from 34% in 2014 (Paulsen, 2016). Small business data breaches affect organizations and are a direct entrance for cyber criminals to gain illegal access into larger corporations (Paulsen, 2016). Data breaches of small businesses also compromise consumers' private information. Despite the number of attacks against small businesses, some small business owners continue to fail to implement the strategies to protect their data (U.S. Department of Homeland Security, 2015b).

Despite the suggestions and importance of protecting data security breaches, some small business owners fail to implement cybersecurity protection because of a lack of knowledge (U.S. Department of Commerce, 2016b). The U.S. Department of Commerce (2017a) acknowledged that most small business owners are not experts in all aspects of securing their systems. More than 50% of small business owners cannot handle cybersecurity threats successfully (U.S. Department of Homeland Security, 2015b). Approximately 41% of small business owners have an insufficient number of resources to secure their data and systems (U.S. Department of Homeland Security, 2015b). Lack of knowledge and resources hinders a small business from advancing (U.S. Department of Homeland Security, 2015b).

Customers demanding cashless payments influenced credit card payments (Clapper & Richmond, 2016; Frazer, 2016). For large businesses, the main point of sale has been through credit card payments, with as much as 66% of all transactions made through credit card payments (Davidson & Turmel, 2017). Among small businesses, the use of credit cards has not reached the same prevalence (Davidson & Turmel, 2017). Small business owners' main point of sales remains rooted in the use of cash registers, but more small business owners are in the process of accepting credit card payments (Davidson & Turmel, 2017). While still using cash registers, small business owners are in the initial stages of transitioning from a predominantly cash register method point of sale to credit card payments (Frazer, 2016).

For those that have already accepted credit card payments, one area of susceptibility regarding data security among small businesses is the lack of protection in their points of sale (Clapper & Richmond, 2016). Dishonest employees having access to cash registers pose a threat to data security (Frazer, 2016). As recommended by the

Payment Card Industry Data Security Standard, all businesses that use a credit card as the point of sale for payment transactions are encouraged to have automatic antivirus software, regular self-assessment, security plan, and network evaluation (Clapper & Richmond, 2016).

The point of sale of small businesses is an access point for hackers because these small business owners also collect information from their customers through their credit card payments (Karanja & Rosso, 2017). The interconnected relationship between small and large businesses from the perspective of hackers underscores the importance of protecting the point of sale of small businesses (Clapper & Richmond, 2016). From these points of sale, in addition to credit card information, hackers can also steal data such as names, email addresses, phone numbers, and addresses (Karanja & Rosso, 2017). This information equips hackers to gain access to various protected websites (Karanja & Rosso, 2017).

The National Institute of Standards and Technology (NIST) offered security information to small business owners to teach them how to protect their data against cyber attacks (U.S. Department of Commerce, 2016b). Data breaches in small businesses impact the economy, particularly the stock market (Smith, Jones, Johnson, & Smith, 2019). Despite these suggestions for enhanced security measures, many small businesses continue to have weak data security infrastructure because of limited resources and lack of awareness and recognition about their importance (Clapper & Richmond, 2016). The NIST suggested that small business owners secure their wireless systems as well as their telecommuting communications (U.S. Department of Commerce, 2016b). NIST also provided guidelines for securing electronic emails (U.S. Department of Commerce, 2016b). To assist small business owners, the NIST also developed eScan to test the security methods implemented by small business owners (U.S. Department of Commerce, 2016b).

The NIST developed the eScan Security Assessment tool as a security strategy to inform small business owners about their information technology systems (U.S. Department of Commerce, 2016b). Information technology personnel can use the system to identify the level of protection against cyber attacks (U.S. Department of Commerce, 2016b). Small business owners use the eScan Security Assessment tool to obtain a series of security questions to test the level of protection within their companies (U.S. Department of Commerce, 2016b). The series of questions included information on contingency plans, security policies, and system failure policies (U.S. Department of Commerce, 2016b). NIST used eScan to provide a report that offered the small business owners the results of the questionnaire with suggestions on data security improvement (U.S. Department of Commerce, 2016b).

While investing in cybersecurity could improve organizational performance, most small business owners fail to invest in the security tools needed to protect their data (Gordon et al., 2018; Gordon, Loeb, & Zhou, 2016). Some leaders fail to invest in cybersecurity protection because the investment does not return an immediate profit (Gordon et al., 2018). The cybersecurity investment is the preventable cost of a future cyber incident (Gordon et al., 2018). Leaders also fail to invest in data security because they are unable to account for the savings that leaders can accrue from implementing cybersecurity (Gordon et al., 2018). The frequency and changes in cyber attacks influence many leaders to wait and see how to protect their data (Gordon et al., 2018). Delaying the implementation of security methods could increase the chance of the leaders experiencing a security breach (Gordon et al., 2018).

When small business owners do not adopt a reliable security measure, infrastructure, or policy, several legal and financial implications are likely to affect their organization (Aguilar, 2015). For instance, small business owners neglecting to implement data security practices properly could also receive a fine by the Federal Trade Commission [FTC] (West, 2017). The FTC intervened on behalf of the customers and filed cases against companies for not adequately protecting consumers' data (U.S. Department of Commerce, 2016b). Each settlement ordered by the FTC could result in 20 years of costly and time-consuming remedial data security processes (West, 2017).

Implementing Policies and Procedures to Prevent Data Breaches

Securing data is a challenging and continuous process for business leaders (Deane, Goldberg, Rakes, & Rees, 2019; Veleva, 2019). Failure to comply with or implement information security policies and procedures may cause business leaders to experience a security breach (Hina, Panneer Selvam, & Lowry, 2019; Rajab, & Eydgahi, 2019; Safa, Solms, & Furnell, 2016). The development and implementation of formal policies are necessary to protect organizational data (Culnan, 2019). These policies and procedures need to evolve to address the rapid changes in data security threats (Schatz & Bashroush, 2019).

Data breaches occur because of a user’s failure to comply with information security policies (Cram, D, & Proudfoot, 2019). Employees pose the greatest threat to organizations (Cram et al., 2019). Information security officers should plan to implement methods, such as policies and procedures, to protect their data (Peltier, 2016).

Employees not adhering to information security guidelines may place the organization at risk (Ifinedo, 2016; Sebescen, & Vitak, 2017). Awareness and education among employees contribute to effective data security strategies (Bada & Nurse, 2019; Kim, Kim, Hong, & Oh, 2017). Parsons, McCormac, Butavicius, Pattinson, and Jerram (2014) published a qualitative study on the knowledge of employees regarding their organization’s security policies and procedures. The study consisted of 500 Australian employees. Parsons et al. indicated that the knowledge of policy and procedures had a stronger influence on employee attitudes toward policies and procedures than self-reported conduct. Training and education were more effective than policies and procedures. The employees could be more engaged in training as opposed to reading policies and procedures (Parsons et al., 2014).

Employee behavior toward policies and procedures may also affect reliable data protection (Merhi & Ahluwalia, 2019). Writers of Internet policies intend to influence employees to use the Internet for work-related activities (Li, Luo, Zhang, & Sarathy, 2018). Li et al. (2018) concluded that employees’ intent to comply with the Internet policies influenced Internet abuse and the costs of noncompliance, with proper sanction risks and possible Internet security risks. Li et al. indicated that employees took more risk if the perceived that their reasons for using the internet could be defended (Li et al., 2018). The lack of self-control also influenced the employees to make poor decisions (Li et al., 2018).

Similar to Li et al. (2018), Vance, Siponen and Pahnila (2012) conducted a study regarding the influence of habitual employee behavior and information systems security. Vance et al., used protection motivation as a theoretical lens and found that employees' habits influenced their decision to comply with information security policies. Employees' habits influenced a positive response from the employees' decision to comply based on the level of the threat. Vance et al., also discovered that system vulnerability did not affect an employee's decision to comply with information system policies.

Managers should enforce the creation and use of access control policies, procedures to contribute to the success of improving data security (Zhao, Wu, Hong, & Sun, 2019). Organizational leaders could implement security policies and procedures for access control, and much more (Peltier, 2016). Organizational leaders use control frameworks to establish internal controls to decrease risk. Access control policies are auditable and used to control authorized access to networks (Zhao et al., 2019).

Business leaders use empirical support when implementing policies and procedures to prevent data breaches (Ifinedo, 2016). Aurigemma and Mattson (2017) conducted a study on governmental employees and their behaviors towards complying with information security policies and procedures. Aurigemma and Mattson asserted that an employee's rank could influence the outcomes of resources and results of others within the organization. Aurigemma and Mattson indicated that while researchers have identified the use of security policies as a valid data protection technique, many organizations have yet to adopt the idea that an employee’s rank could influence their decision to comply with the rules.

Similar to Aurigemma and Mattson (2017) study, Ifinedo (2016) conducted a study to determine the importance of the guidelines for information systems security policies. Ifinedo indicated that an employee’s rational choice influences the noncompliance or compliance to adhere to security guidelines. Managers should find more creative and proactive methods to display the importance of information security guidelines (Ifinedo, 2016). While the majority of the researchers in the literature indicated that the implementation of a robust security policy in organizations is essential (Ifinedo, 2016), some have found no support for such claims.

Researchers Al-Alawi, Al-Kandari, and Abdel-Razek (2016) would disagree with the importance of implementing information security policies. Al-Alawi et al. published a study on the influence of information security policies on data security breaches in Kenya public universities. Al-Alawi et al. indicated a weak relationship between security policies and security breaches. According to Al-Alawi et al., information security policies have little influence in reducing security breaches.

Business leaders use security policies to identify the roles and responsibilities of the employees to protect the systems in their organization (Ifinedo, 2016). Leaders implement security policies and procedures to address electronic communication standards, data protection, code of conduct, and physical security (Cram et al., 2019). While leaders design data security policies and procedures to protect the information, most policies and procedures are not comprehensible by most readers (Das, Cheung, Nebeker, Bietz, & Bloss, 2018). Users review policies to identify the risk they are taking to use a product or service (Das et al., 2018). Business leaders should store the policies in a location so that users can later refer to the policies if they have concerns about how companies are utilizing their information (Das et al., 2018). Users are required to sign an electronic agreement to access web-based and digital tools (Das et al., 2018). Leaders should implement a training mechanism to educate users on the possibility of risking private information (Das et al., 2018).

In conclusion, implementing and using policies and procedures may assist business leaders in avoiding a security breach (Ifinedo, 2016; Peltier, 2016). Employees' personal norms may influence their behavior toward complying or not complying with data security policies and procedures (Li et al., 2018; Vance et al., 2012). Organizational leaders should continue to find more ways to implement the appropriate policies and procedures to protect the business and consumers (Das et al., 2018). The next section is a discussion of the different strategies that leaders used to protect and secure organizational data.

Strategies to Protect Organizational Data

Organizational leaders use various strategies to protect organizational data from hackers who are intending to steal valuable information (Demay, Gaži, Maurer, & Tackmann, 2019). Some of the most common data security strategies include passwords, employee education, data back-ups, and Bring Your Own Device (BYOD) system. In this section, I discussed the extant literature on these four data security strategies.

Password. Passwords are a highly used method to protect a system (Butler & Butler, 2018). Weak passwords are vulnerabilities to a system (Brumen, 2019; Demay et al., 2019). While many sophisticated techniques protect data from unwanted intruders, password protection remains a standard method (Demay et al., 2019). Passwords are a means to prevent hackers from stealing an individual's or an organization's private information (Boiko & Shendryk, 2017).

Weak passwords are common approaches that leaders and employees use to access protected computer-based systems (Demay et al., 2019). Users struggled to remember strong passwords (Guo, Zhang, & Guo, 2019). Hackers were able to hack systems were users chose weak passwords (Guo et al., 2019). Weak passwords are less than eight characters and do not contain upper case and lowercase letters, numbers, and nonalphanumeric symbols (Allen, 2014).

Whitty, Doodson, Creese, and Hodges (2015) published an article on the human behavior of cyber security and passwords. Whitty et al. discussed the risky practices of sharing passwords. Whitty et al. initially believed that older internet users were riskier with choosing passwords. Whitty et al. later found that younger users were more likely to share passwords across multiple platforms (Whitty et al., 2015). While users were educated and aware of good password practices, they still chose to make poor cyber security decisions.

User's implement password vaults to store passwords to prevent the user from forgetting passwords (Allen, 2014; Chaudhary, Schafeitel-Tähtinen, Helenius, & Berki, 2019). However, these password managers can be prime targets for hackers, given the scope of confidential information in these vaults (Chaudhary et al., 2019). Hackers could compromise a user's account by breaking into an account with the weakest system (Allen, 2014). Users should avoid writing down common words and numbers, as well as passwords (Allen, 2014). Writing down passwords and forgetting passwords are common user behaviors that compromise password security (Allen, 2014). Hackers may experience a challenge when the keys to the password vault are securely stored (Allen, 2014).

Woods and Siponen (2018) conducted a study on password memorability. Woods and Siponen suggested that users forget passwords because of memory limitations. Users also create vulnerabilities by reusing the same password for access to different applications (Woods & Siponen, 2018). Inadequate password habits may be a result of the user's ability to reset their passwords. While users have practiced unsafe habits with securing their passwords additional research should be done to determine if users are not complying with password policies because of memory limitations.

Catuogno and Galdi (2014) suggested that alphanumeric passwords and pin-based authentication have disadvantages. Catuogno and Galdi conducted a study evaluating the authentication of security by using an SAT-based attack. Catuogno and Galdi implied that the use of graphical passwords is becoming popular. Applying graphical passwords on small devices requires quality equipment to display images and maintain proper data storage (Catuogno & Galdi, 2014). Graphical passwords may overcome the drawbacks discovered when using passwords and pin-based authentication (Gi-Chul, 2019; Juneja, 2020; Nizamani, Hassan, Shaikh, & Bakhsh, 2019). Implementing a graphical password scheme is affordable and beneficial to organizations (Catuogno & Galdi, 2014). Other types of nonalphanumeric password schemes include multifactor authentication, passwords, fingerprints, and iris-scans (Catuogno & Galdi, 2014; Ribeiro et al., 2019).

Contrary to Catuogno and Galdi (2014), Renaud, Otondo, and Warkentin (2019) claimed that human behavior contributed to an individual's reluctance to comply with password policies and procedures. IT leaders host summits and training classes to change the behavior of the recipients (Renaud et al., 2019). Trainers design these courses to influence proper data security behaviors (Renaud et al., 2019). However, some recipients return to their normal habits of using inadequate passwords (Renaud et al., 2019). Researchers have not been able to identify the reasons that cause individuals to reject security advice (Renaud et al., 2019). While the reasons are unknown, security leaders should continue to search for explanations and provide interventions to reduce resistance from individuals who fail to comply with security rules (Renaud et al., 2019).

Similar to Renaud et al. (2019), Campbell, Ma, and Kleeman (2011) examined the influence of restrictive password composition policy. Campbell et al. (2011) used Levenshtein's distance approach and revealed the enforcement of restrictive password composition. There was a significant increase between common dictionary words and user-selected passwords. Organizations should educate users on the risk of weak passwords (Campbell et al., 2011).

With the proliferation of technology, users' methods of communication have also evolved (Muthumeenakshi, Reshmi, & Murugan, 2017). Developers have created authentication methods such as a three-party password-based authentication key

(Muthumeenakshi et al., 2017). The authentication key allows users to create a shared cryptographic key from a trusted server to create a common key among the users sharing the server (Muthumeenakshi et al., 2017). The key blocks hackers from intercepting the communication using a dictionary attack (Muthumeenakshi et al., 2017). This process enables users to communicate over a public network securely (Muthumeenakshi et al., 2017).

Nam, Kim, Choo, and Paik (2013) reviewed a version of the three-party PAKE protocols developed by Gao, Ma, Guo, Zhang, and Ma (2013). Nam et al. criticized Gao et al.'s work for its vulnerability to unpublished offline and online dictionary attacks by hackers. Nam et al. proposed that developers should (a) verify the keying materials received by the client from the server, (b) ensure the open group does not generate a password entangled protocol message, and (c) confirm that the users send at least one authenticated message to the server. Key exchange is a method where a shared high-entropy key becomes available to two or more parties for subsequent cryptographic use (Allen, 2014). Word-based authenticated key exchange (PAKE) protocols are a type of key exchange protocols that allow two or more parties to communicate in a public network to generate a session key from their low-entropy passwords. Low-entropy passwords are easy for individuals to remember (Allen, 2014). A central challenge in designing a PAKE protocol is to prevent dictionary attacks, in which an attacker systematically computes all possible words to find the correct word to infiltrate the system (Allen, 2014). Based on these findings, information technology leaders can improve password use by implementing a two-factor authentication process wherein users need to perform two interrelated verification tasks. Two-factor authentication is a process used to confirm a user’s identity after successfully presenting two pieces of evidence through an authentication mechanism (Esiner & Datta, 2019).

In conclusion, passwords are the most common security measures that organizational leaders used to protect their data from intrusion from hackers (Demay et al., 2019). If effectively used, passwords can prevent hackers from stealing an individual’s or an organization’s private information (Campbell et al., 2011). Based on the research studies that I reviewed in this section, passwords are more effective when they are complex. Password security should include nonalphanumeric methods, and the application of a two-step authentication process (Nam et al., 2013).

Employee education. Organizational leaders can reduce data security breaches by adequately training employees (Caldwell, 2016; San Nicolas-Rocca, & Burkhard, 2019). Implementing training is ineffective without a follow-up plan to ensure that the original training plan is working (Caldwell, 2016). Creating interactive training with real-life scenarios is beneficial because employees tend to ignore online training with unrealistic examples (Caldwell, 2016). The lack of interest in the training may cause employees to click through training without reading the material (Caldwell, 2016).

Caldwell (2016) examined the nature of cyber attacks that occurred in the company Mimecast. Caldwell indicated that 25% of the participants admitted they do not frequently train employees to detect email cyber attacks, while less than 10% stated they test employees every month. Based on these findings, leaders should tell employees how to prevent cyber attacks with their personal and work devices to increase security awareness (Caldwell, 2016). IT officers should set employee security training according to the employees’ privileges within the organization. Employees who are responsible for protecting the IT infrastructure should be required to take additional training.

Training has become a governmental regulation for some companies (FTC, 2015). The FTC has accused companies such as MTS, TRENDnet, and HTC America of not training their engineers regarding the proper coding practices that can enhance data security in organizations (FTC, 2015). Training the engineers to improve the security of the software code can also improve the data security of an organization (Ahmed, Latif, Latif, Abbas, & Khan, 2018). Failure to use secure coding practices could allow malicious intruders to communicate with applications.

Data backups. Data backups are a data security strategy that organizational leaders can use to protect and recover data (U.S. Department of Homeland Security, 2016). Data backups are also digital libraries that house sensitive information. If business leaders perform data backups, information is retrievable in case of data loss or breach (Singh, 2019). Business leaders should choose data backup methods based on security and business needs (U.S. Department of Homeland Security, 2016). Organizational leaders collect massive amounts of data to function in daily processes (U.S. Department of Homeland Security, 2016). Data backups allow leaders of organizations to prevent a disruption in service, facilitating the restoration of data after a malicious or unintentional software of hardware failure (Chuang & Wang, 2017). Depending on the type of business, the federal government or the business leaders may have regulations implemented that requires the organization to implement data back-ups regularly (Gozman & Willcocks, 2018).

While developing a plan about what to restore this process is encouraged by IT leaders, knowing how to store the data for the backup process is also critical (Chang, 2015). IT leaders should add a data backup to the contingency plan of the organization (Chang, 2015). Implementing a data backup process could save business leaders from data disasters and save time with data restoring efforts because data backups are critical to restoring data within an organization (Chang, 2015). Business leaders should begin the data backup process by identifying the type of data on the network and the company devices that employees use. Users should scan hard copies of data for digital scanning (U.S. Department of Homeland Security, 2015a). Digitally scanning data creates a format of data storage, allowing IT leaders to back up the information (U.S. Department of Homeland Security, 2015a).

Business leaders should discuss the type of security and type of storage device when developing the contingency plan (U.S. Department of Homeland Security, 2015a). The security level of the data backups should be equal to the original level of security on the primary source of data (U.S. Department of Homeland Security, 2015a). IT leaders should accompany back up plans by a business effect analysis to evaluate the possibility of lost data (U.S. Department of Homeland Security, 2015a). Selecting the proper storage device may vary based on the type of organization (U.S. Department of Homeland Security, 2015a). IT leaders can store data on cartridges, USB drives, and other saving devices with integrated data backup software (U.S. Department of Homeland Security, 2015a).

To prevent loss of data, some businesses back up the data using cloud storage or a server in a different location from the original data (U.S. Department of Homeland Security, 2015a). Cloud storage is cost-efficient and popular in an organization's IT infrastructure (Ramachandran & Chang, 2016). According to Attaran and Woods (2018), cloud-computing technology provides both small and large business organizations a convenient way to back up storage space on the Internet. While cloud storage is a viable solution to store data, the open nature of cloud-computing storage poses several security challenges that may include service traffic hijacking, network security issues, potential massive outages, and malicious insider activities (Annane, & Ghazali, 2019).

Chang (2015) published an article on disaster recovery in a private cloud, which is virtual storage. Virtual storage is easily accessible from any place in the world that has network connections (Liu, Liang, Susilo, Liu, & Xiang, 2016). Chang recommended businesses to use multiple methods to back up data. Instead of focusing on data security and privacy, Chang took a different approach with his research by focusing on the disaster recovery process for big data systems. Implementing a single method of disaster recovery could cause an organization to fail with recovering data, whereas restoring data in multiple locations increases the chances of achieving data recovery in the case of a system failure (Chang, 2015). The performance of different disaster recovery approaches is different from each other (Chang, 2015). Chang found that while using multiple disaster recovery methods in all data centers, business leaders could recover one terabyte of data in approximately 650 seconds for a single site while recovering one terabyte of data in approximately 1,360 seconds for three sites.

Organizational leaders also need to secure data back-ups. Allen (2014) published a study involving lawyers and data backup practices in their respective firms. Allen had an approach similar to researchers such as Park, Kim, Park, Lee, and Kim (2019) who also focused on the encryption process for data backup. Allen implied that a reliable disaster recovery plan, such as the use of backups in another server, could be necessary in times of data security catastrophe.

Information technology and organizational alignment. One issue pertinent to the principles of systems theory is the importance of organizational alignment, which affects the performance of companies. For instance, some business managers believed that the alignment of information technology strategies and business strategies influenced organizational performance (Reynolds & Yetton, 2015). Small business owners are challenged with the alignment of technology within their organizations because of their lack knowledge and resources (Wang & Rusu, 2018).

Reynolds and Yetton (2015) explored a study on aligning business and IT strategies in multi-business organizations. In the findings, Reynolds and Yetton found that IT functional, structural, and temporal alignments had a positive effect on organizational performance. Functional alignment had a positive effect on organizational performance when IT competencies complemented business and IT capabilities (Reynolds & Yetton, 2015). Structural alignment had a positive effect on organizational performance based on IT governance (Reynolds & Yetton, 2015). The performance driver for temporal alignment occurred when IT flexibility was present (Reynolds & Yetton, 2015).

Similar to Reynolds and Yetton (2015), Gerow, Thatcher, and Grover (2015) studied intellectual and operational alignment in organizations. Gerow et al. found that intellectual alignment had no significant direct effect on financial performance between IT and business alignment in the technology transformation and potential competitive alignment. Gerow et al. also found that IT alignment did not have a direct effect on financial performance through operational alignment. Intellectual alignment is apparent when managers align IT and business strategies, whereas operational alignment occurs when managers align IT, business processes, and infrastructure (Gerow et al., 2015).

Bring your own device. Bring Your Own Device (BYOD), sometimes referred to as consumerization, is the process in which organizational leaders allow employees to use their devices for work-related activities (Zahadat, Blessner, Blackburn, & Olson, 2015). As referenced by de las Cuevas and Peñate (2015), IBM was the first organization to support the adoption of BYOD. Sometimes employees decide to use their own devices regardless of the recommendations of IT leaders (Leclercq-Vandelannoitte, 2015). Employees enjoyed BYOD because of job flexibility, control, and technology empowerment (Zhang, Mouritsen, & Miller, 2019). As a result, BYOD has offered organizations cost savings, job satisfaction, and productivity (Zahadat et al., 2015).

Organizational leaders use BYOD policies to assist in protecting their data (Vignesh & Asha, 2015). Bradford Networks recommended a 10-step process for developing a BYOD strategy (Mansfield-Devine, 2012). The 10-step process included selecting the devices, OS version, applications, and groups of employees (Mansfield-Devine, 2012). The 10-step process also included inventory authorization for users and devices, network access, employee education, and continuous vulnerability assessment (Mansfield-Devine, 2012).

Outside the IT staff, employees can also play an essential role in protecting company data (Mansfield-Devine, 2012). Managers should include employees in the development of their security plans (Mansfield-Devine, 2012). BYOD is a strategy that gives employees a central role in data security in organizations (Baillette & Barlette, 2018; Dhingra, 2016). According to Cho and Ip (2018), employees are more likely to adopt BYOD when the perceived job security is high or when organizational commitment is high.

While this concept of BYOD is trending, some information technology officers fear the security risks that leaders can experience because of adopting this security strategy (Baillette & Barlette, 2018). BYOD allows employees to access personal information and work information interchangeably from personal devices such as phones, laptops, and tablets, while connected to the organization's network (Dhingra, 2016). To decrease the security risks, Leclercq-Vandelannoitte (2015) recommended organizational leaders to reconsider their security process, models, and practices to include strategies to deal with BYOD rather than miss opportunities because of their lack of participation in this new security method. As referenced by Dhingra (2016), Gartner predicted approximately 50% of employers would want employees to use their own devices by

2017. An additional study conducted by Juniper Research suggested organizational leaders would implement more than one billion devices for BYOD purposes by 2018.

Despite recommendations by researchers such as Mansfield-Devine, some companies refuse to entertain the idea of BYOD (Leclercq-Vandelannoitte, 2015). Instead, information security officers have banned employees from connecting personal devices to the organization's network and have prohibited employees from conducting work on their devices to avoid security concerns (Leclercq-Vandelannoitte, 2015). Personal devices may pose a threat to organizational systems (Astani, Ready, & Tessema, 2013)

Organizations that allowed BYOD were facing a significantly high rate of security threats (Crossler, Long, Loraas, & Trinkle, 2017). The threats include malware and the security of company information (Astani et al., 2013). Some data leaks are unintentional wherein employees may inadvertently connect to a company network and inadvertently put the organization's network at risk by downloading files from the Internet and saving them to a local hard drive (Morrow, 2012). Branch et al., 2019 reported an increase in malware attacks. Malware retrieves personal information from the device for financial gain for the intruder. Information security officers should be concerned with intruders finding backdoors to access the organization's data (Branch et al., 2019). Organizations must develop security programs to address concerns with BOYD devices; otherwise, organizations risk employees intentional or unintentionally leaking private information to outside individuals (Astani et al., 2013).

Organizational leaders who are using BYOD should include a cross-functional team of IT security and users when developing a robust data security plan (Mansfield-Devine, 2012). The use of security policies can ensure the network is locked down with access controls constructed on who, what, and where (Mansfield-Devine, 2012). Knowing who is on the network and where and what items are on the network equips IT security with the knowledge to develop a more sophisticated BYOD policy (Mansfield-Devine, 2012).

Consistent with the recommendation of Mansfield-Devine (2012) regarding the need for a cross-functional security planning, Vignesh and Asha (2015) suggested that BYOD security policies should include organizational level, device level, and application level in the data strategy policy. The organizational level includes an agreement by the employee to follow the policy as well as control employee access for devices (Vignesh & Asha, 2015). Security leaders use the device level to monitor certificate authority and encryption (Vignesh & Asha, 2015). The application level consists of mobile content management, such as monitoring the applications on the device and controlling permissions (Vignesh & Asha, 2015).

Similar to Vignesh and Asha’s (2015) recommendations regarding BYOD security policies, Mansfield-Devine (2012) stated that organizations should consider the authentication of the user and the device. According to Morrow (2012), approximately 70% stated that mobile device management is essential. Morrow suggested that security officers should plan beyond authorized and unauthorized users. The data protection process should start at the storage level and continue from transport to delivery (Morrow, 2012). IT officers should set rules to control device-based apps on the network by using mobile device management (Morrow, 2012).

Vignesh and Asha (2015) took their research a step further and discussed the importance of maintaining certificate authority credentials on BYOD devices. Users have become more educated when using devices by adding and deleting certificate authority credentials and jailbreaking phones without assistance (Vignesh & Asha, 2015). Maintaining certificate authority control by the IS security officers may reduce unwanted data leakages (Vignesh & Asha, 2015). Users may share some security responsibilities (Vignesh & Asha, 2015). IS security should request users to encrypt SD cards to reduce data security issues when a device is lost or stolen (Vignesh & Asha, 2015).

Jailbroken devices, which contain illegally downloaded software, may also pose a threat to an organization because hackers can write malware to steal data (Morrow, 2012). These devices with illegally downloaded software allow users to access administrative privileges to download illegal applications capable of leaking sensitive data (Vignesh & Asha, 2015). Morrow (2012) suggested that organizations should not focus on distinguishing between personal and organizational devices. Instead, IS organizations should concentrate on protecting the data (Morrow, 2012). Hackers seem to attack more Android devices versus Apple or Linux (Morrow, 2012). Apple’s platform is not open (Morrow, 2012). Android has an open platform, which makes it vulnerable to more attacks on its applications (Morrow, 2012).

Given the security issues pertinent to the adoption of BYOD in organizations, de las Cuevas and Peñate (2015) conducted a study about corporate security solutions for

BYOD. De las Cuevas and Peñate used the multi-platform usable endpoint security (MUSES) framework. MUSES is a tool that leaders used to reduce and manage security risk in a BYOD environment by tracking users' behavior regarding data security (de las Cuevas & Peñate, 2015). Systems administrators can use MUSES to control user's device rights for their private and corporate use (de las Cuevas & Peñate, 2015). Users' past behavior determines the rules applied to control their access. MUSES is a unique tool that allows IS security officers to implement security policies for insider threats versus attacks from external intruders (de las Cuevas & Peñate, 2015). While external attacks can be detrimental to an organization, insider attacks are the top data security issues (de las Cuevas & Peñate, 2015). MUSES differ from most tools on the market for BYOD. MUSES support more than the common BYOD tools; it also includes an organization's PCs and laptops (de las Cuevas & Peñate, 2015). While MUSES covers many security threats, MUSES is unable to create rules to detect unknown or unexpected threats (de las Cuevas & Peñate, 2015).

IS security officers should implement tools based on the type of protection they are trying to achieve (de las Cuevas & Peñate, 2015). Security officers should also create rules to detect online and offline threats before issuing the device (de las Cuevas & Peñate, 2015). Offline detection methods do not allow modifications to the rules after issuing the device (de las Cuevas & Peñate, 2015). Online threat detection is in real-time (de las Cuevas & Peñate, 2015). Similar to online and offline threat detection, security officers should create device management rules by using updatable or fixed information (de las Cuevas & Peñate, 2015). De las Cuevas and Peñate recommended the use of firewall protection to protect private cloud storage and threat monitoring. Morrow (2012) suggested that organizations should not focus on distinguishing between personal and organizational devices. Instead, IS organizations should focus on protecting the data (Morrow, 2012).

In conclusion, BYOD can be a useful employee-based data security strategy that organizational leaders can encourage (Zahadat et al., 2015). Organizational leaders should have a robust security plan and policy to ensure that employees are properly securing their BYOD usage (de las Cuevas & Peñate, 2015; Vignesh & Asha, 2015). Some proposed security measures in the use of BYOD include tracking of employee activities and firewall protection (de las Cuevas & Peñate, 2015).

Transition

Many small businesses are susceptible to cyber attacks because of insufficient security plans (Rohn et al., 2016). The specific business problem is that some small business owners lack strategies to reduce data security breaches. The purpose of this study was to explore various strategies small business owners used to reduce data security breaches. The conceptual framework was systems theory (Bertalanffy, 1968), positing that the understanding of an organization should be holistic and cognizant of the interrelatedness of different organizational components and processes.

Organizational leaders use various strategies to protect organizational data from breaches and cyber attacks (Allen, 2014). Some of the most common strategies include passwords, employee education, data back-ups, and BYOD. These data security strategies have advantages and disadvantages, usually requiring proper alignment with the needs of the leaders of business organizations.

Section 1 included an introduction to the background of the study, problem statement, and purpose statement, the nature of the study, the research question, interview questions, and conceptual framework. In addition, I included the assumptions, limitations, and delimitations; the significance of the study; and literature review for the study. Reviewing previous research allowed me to discover what information exists concerning the study. The review of the academic and professional literature also allowed me to compare sample sizes, research methods, and designs.

Section 2 contains an overview of the purpose statement, the role of the researcher, participants, explanation of the methodology, research design, and data collection techniques that I used as the researcher. Population and sampling, ethical research, data collection, data organization, data analysis, and reliability and validity methods conclude Section 2. Section 3 includes an introduction, presentation of findings, application to professional practice, implications for social change, recommendations for action, recommendations for further research, reflections, and conclusion.

Section 2: The Project

The objective of this study was to explore what strategies small business owners use to reduce data security breaches. In Section 2, I present an in-depth explanation of my methodology and research design. Section 2 also includes the (a) purpose of the study, (b) role of the researcher, (c) participants, (d) research method, (e) research design, (f) population and sampling, (g) ethical research, (h) data collection instrument, (i) data collection technique, (j) data organization, (k) data analysis, and (l) reliability and validity.

Purpose Statement

The purpose of this qualitative multiple case study was to explore strategies small business owners use to reduce data security breaches. The targeted population consisted of four small business owners with successful experience in reducing data security breaches. The geographical location of the study was in the southern region of the United States. The study may contribute to positive social change by rebuilding the relationships between business leaders and consumers. Rebuilding relationships between business leaders and consumers could result in increased spending to support local communities and improve the financial health of the local economy (Nguyen et al., 2015).

Role of the Researcher

In qualitative research, the researcher is the primary research instrument (Leedy, Ormrod, & Johnson, 2019; Twining, Heller, Nussbaum, & Tsai, 2016; Yates & Leggett, 2016). The researcher collects and analyzes data to report the findings (Bengtsson, 2016; Roulston, 2016; Yin, 2018). As the primary instrument, my responsibilities were to (a) collect data, (b) analyze data, and (c) report the results and findings. Researchers may decrease their personal bias by sharing their connection to the research (Birt et al., 2016; Loeb et al., 2017; Madill & Sullivan, 2017). My former professional career as a software engineer gave me a personal connection to the study. I have worked as an IT professional for more than 15 years. During my career, I have experienced personal security breaches. I did have a personal association with the potential participants.

To maintain scholarly work, researchers must uphold ethical behavior to protect the participants (Navab, Koegel, Dowdy, & Vernon, 2016; Pearce, Ensafi, Li, Feamster, & Paxson, 2018; Wilson, Kenny, & Dickson-Swift, 2018). The Belmont Report is a summary of the following ethical principles and guidelines (a) review risk-benefit to determine the appropriateness of research involving human subjects, (b) adhere to the guidelines when selecting human subjects for participation, and (c) provide informed consent to participants (U.S. Department of Health & Human Services, 1979b). I adhered to the ethical guidelines recommended in the Belmont Report and comply with the standards of Walden University's Institution Review Board (IRB). I did not work with participants until after I received IRB approval # 09-26-19-0329502.

As the primary research instrument during the data collection phase, my role was to reduce bias and refrain from displaying reactions that may create unbiased opinions from the participants. It is impossible to reduce all bias from research; qualitative researchers can implement member checking, outline the data collection process, and use triangulation to reduce bias in research (Dewasiri, Weerakoon, & Azeez, 2018; Joslin & Müller, 2016; Oleszkiewicz, Granhag, & Kleinman, 2017). In the study, I used member checking, defined the data collection process, and used methodological triangulation to reduce bias. Collecting information outside of the researcher's place of employment may reduce assumptions, unexpected role ambiguity, ethical encounters, and bias (Burns, Fenwick, Schmied, & Sheehan, 2012). To further reduce bias, I did not select participants from my place of employment.

Researchers can mitigate bias by following an interview protocol (Yin, 2018). An interview protocol includes interview questions and a preset script to guide the interviewer through the interview process (Castillo-Montoya, 2016; Mwangi, Chrystal, & Bettencourt, 2017; Parkhurst, 2017). The preset script includes what the researcher will say before, during, and after the interview (Mwangi et al., 2017). I used an interview protocol (Appendix A) to guide my data collection process. The interview protocol helped me keep the schedule and stay focused on the topic.

Participants

Researchers use qualitative methods to provide the readers with a view of the participants' interpretation of their experiences and thoughts about a phenomenon (Comert, 2018; Runfola, Perna, Baraldi, & Gregori, 2016; Sundar, Løndal, Lagerløv, Glavin, & Helseth, 2018). Researchers should select participants relevant to the study to improve data collection and answer the research question (Alexander, Kiernan, Oppezzo, & Resnicow, 2018; Allen et al., 2018; Saunders & Townsend, 2016). To answer the research question, I selected participants who could answer the research question. Participants should have the ability to provide the researcher with reliable access to the data (Saunders & Townsend, 2016). Exploring the strategies used by small business owners contribute to the sustainability of small businesses (Turner & Endres, 2017). Small business owners who maintain a small business for at least 5 years can provide strategies to increase the growth of businesses (Turner & Endres, 2017). Potential participants met the following eligibility requirements (a) own a small business in the southern region of the United States for at least 5 years, (b) employ less than 1500 employees, (c) use technology to conduct business, (d) have implemented data security strategies successfully, and (e) take part in the data security decision-making process to support the business.

After receiving IRB approval, I began the recruitment process. I started by researching directories, Internet searches, tax records, and government websites. I collected a list of potential participants. I did not select any participants from a school/work setting that involves a service provider. Gaining access to participants requires establishing trustworthiness between the researcher and participants, getting consent, and obtaining an agreement (Amundsen, Msoroka, & Findsen, 2017; Bronnenmayer, Wirtz, & Göttel, 2016; Porter, Wilfond, Danis, Taylor, & Cho, 2018). To obtain contact information, I conducted Internet searches and went to business locations for a face-to-face visit. I also contacted participants via mail, email, and phone using a recruitment letter (see Appendix B). The recruitment letter consisted of detailed information describing the purpose of the study. Providing participants with a clear description increases trustworthiness (Leedy et al., 2019).

I mailed 25 letters by U. S. postal service to 11 franchise small business owners and 14 nonfranchise small business owners, and I did not receive any responses. I was able to obtain 17 email addresses out of the 25 potential participants. I was not successful at receiving feedback from the email addresses. I called nine of the potential participants and visited six locations face-to-face before I successfully received four participants. After the potential participants replied with their consent by phone, email, or U.S. postal service, I followed up and established a meeting arrangement and set a deadline for the data collection.

Researchers must be open and honest with participants to build a trusting relationship (Yallop & Mowatt, 2016). Allowing participants to communicate openly can establish a trustworthy environment and promote confidentiality between the interviewer and the interviewee (Connelly, 2016; Gibson, 2017; Yin, 2018). Researchers should reveal the characteristics of the participants to provide the readers with clarification and improve the understanding of the sample (American Psychological Association, 2010). To align with the research question, I purposefully selected small business owners who have successfully implemented strategies to protect the data within the organizations. The participants selected for the study represented a variety of social and economic backgrounds. All small business owners were 21 years of age and older. The participants were in business for at least 5 years as a small business owner.

Research Method and Design

I used the qualitative method with the case study design to explore the strategies small business owners use to reduce data security breaches. The following section is an extension of the Nature of the Study subsection presented in Section 1. This section is a more in-depth explanation justifying the selected methodology and design.

Research Method

Qualitative research is an acceptable research method in the academic community (Bailey, 2014). I chose the qualitative study to explore the strategies small business owners use to reduce data security breaches. My review of previous studies related to small business strengthened my decision to use a qualitative method. Qualitative researchers gain a rich understanding of a phenomenon (Andrews, No, Powell, Rey, & Yigletu, 2016; Athukorala et al., 2016; Cornelissen, 2017). The exploration allowed me to understand multiple realities of the phenomenon. Researchers have demonstrated qualitative approaches are valuable research tools when used to create meaningful business decisions (Bailey, 2014; Sukamolson, 2016; Taguchi, 2018). Qualitative researchers explore the experiences of the participants (Yin, 2018). The themes that emerged from the study were the perceptions and experiences of the participants.

Quantitative researchers seek to use experimental methods measured by statistical data used to address the research question (Counsell, Cribbie, & Harlow, 2016; Fàbregues & Molina-azorín, 2017; Leedy et al., 2019). In quantitative research, researchers derive the theory before the analysis of the data. Quantitative researchers depend on the ability to generalize from a sufficient sample (Leedy et al., 2019). A quantitative method was not sufficient to satisfy the research question. Researchers use quantitative methods to support testing specific hypotheses about cause-and-effect relationships (Leedy et al., 2019). The qualitative method was more appropriate than a quantitative method for the study because I desired to explore the phenomenon in-depth by using a smaller number of participants.

The mixed method was not appropriate because applying it to the study would increase the amount of time required to conduct the study and integrating both methods is difficult. Strengths and weaknesses are present in mixed methods research (Almalki, 2016; Maxwell, 2016; Molina-Azorin, Bergh, Corley, & Ketchen, 2017). The mixed method can increase the amount of data on the topic while increasing the amount of time and cost required for research (Almalki, 2016; Rahman, 2016). Researchers implementing a mixed method approach may have trouble during integration (Molina-Azorin et al., 2017). Mixed method researchers may risk corrupting data by not considering proper assumptions, rules, and bias behaviors (Bazeley, 2016). Lack of knowledge of both qualitative and quantitative may also create more problems for the researcher and the validity of the research (Bazeley, 2016).

Research Design

Defining the research question is essential when selecting the research design (Yin, 2018). I used a case study design to answer the research question. A case study design answers *how*, *what*, and *why* questions (Yin, 2018). The overarching research question for the study was as follows: What strategies do small business owners use to reduce data security breaches? Researchers use case studies when the boundaries between the context and the phenomenon are not clearly defined (Yin, 2018). The use of multiple sources of data strengthens a case study (Abdalla, Oliveira, Azevedo, & Gonzalez, 2018; Mauceri, 2016; Olivier, 2017). I chose the case study design to add to the existing literature on the business leader’s decision-making for data security.

Knowledgeable qualitative researchers have recognized case study research as an independent qualitative approach to research (Yin, 2018). Several prominent researchers of qualitative case studies who are experts in the field have encouraged the use of case studies in research. For instance, Yin (2018) reviewed the case study design from a post-positivist viewpoint. Merriam and Tisdell (2016) reviewed case studies using a social constructivist pattern.

The phenomenological design is an interpretation of the participants' lived experiences of a phenomenon that focuses on the individual and not the factors that influence a phenomenon (Dodgson, 2017; Ferreira & dos Santos, 2016; Gauche, de Beer, & Brink, 2017). The purpose of phenomenological research is to understand the meaning of an experience not to generalize the phenomenon (Gauche et al., 2017). Phenomenological research was not appropriate for the study because I was not using a focus group to explore the lived experiences of the participants.

A researcher using a narrative research design can analyze individuals and their experiences with a phenomenon (Kourti, 2016; Ross, Iguchi, & Panicker, 2018; Yin, 2018). The researcher attempts to capture data based on a storytelling session in which the participants' express their lived experiences (Graci & Fivush, 2017). A narrative method was not appropriate for this study because of the extensive information needed from participants. Researchers using narrative research experience issues in collecting and analyzing data. For example, narrative researchers ask the following questions: Who is telling the story? Who can tell a story? A narrative design also involves storytelling from the participants and the researcher could introduce biased information (Graci & Fivush, 2017).

A researcher using the ethnographic research design analyzes multiple individuals who reside in the same place and share the same beliefs and language (Bamkin, Maynard, & Goulding, 2016; Hoolachan, 2016; Luborsky & Lysack, 2017; Sharp, Dittrich, & deSouza, 2016). This design allows the researcher to study a culture sharing group (Bamkin et al., 2016). Unlike a case study, the ethnographic design is appropriate when the researcher’s goal is to explore and understand how groups and cultures work (Cappellaro, 2017). I did not choose the ethnographic design because I was not focusing on the culture of the organization, and the participants do not live in the same place or share the same beliefs.

In qualitative research, the researcher reaches data saturation when no new information is available (Boddy, 2016; Carmichael & Cunningham, 2017; Jin, Pang, & Smith, 2018). Researchers may reach data saturation in qualitative research, where interviews are the primary source of data collection (Marshall & Rossman, 2016). For this study, I interviewed participants until redundancy and repetition appear in the data.

Population and Sampling

Purposeful sampling is the most commonly used sampling method for qualitative research (Benoot, Hannes, & Bilsen, 2016; Chandani et al., 2017; Etikan, Musa, & Alkassim, 2016). A purposeful sample is a small selection of a larger population (Etikan et al., 2016; Yin, 2018). I used a purposeful sample to address the research question; initial participants may provide contact information for additional participants who meet the purposeful sampling criteria. In qualitative research, researchers apply professional judgment when selecting participants who can best answer the research question (Merriam & Tisdell, 2016).

Researchers reach data saturation when no new themes emerge from the data (Carmichael & Cunningham, 2017; Jin et al., 2018; Yin, 2018). Qualitative researchers increase their chances of reaching data saturation when choosing the appropriate sample size (Boddy, 2016). Researchers reach data saturation from using purposeful samples and interviewing participants (Bungay, Oliffe, & Atchison, 2016; Carmichael & Cunningham, 2017; Sperandei, Bastos, Ribeiro-Alves, & Bastos, 2018). Data saturation is also when the researcher selects participants with similar experiences (Fusch & Ness, 2015). Failure to achieve data saturation adversely influences the validity of the study (Fusch & Ness, 2015). I purposefully selected four participants and continued to ask them questions until no new themes emerge.

Researchers should seek a minimum of four to 15 participants to obtain thick and rich data (Onwuegbuzie & Byers, 2014). Researchers choose a smaller population to achieve a need or purpose (Etikan et al., 2016; Yin, 2018). I continued to solicit participants until I recruited four small business owners.

The population comprised of four small business owners who met the participant criteria: (a) owned a small business in the southern region of the United States for at least 5 years, (b) employed less than 1500 employees, (c) used technology to conduct business, (d) had implemented data security strategies successfully, and (e) take part in the data security decision-making process to support the business. The participants also used electronic transactions to conduct business. The approximate number of small business owners within the study’s population is 254,598 (U.S. Department of Small Business Administration, 2018).

Qualitative researchers use interviews to collect rich data (Kallio, Pietilä, Johnson, & Kangasniemi, 2016; Kara & Pickering, 2017; Marshall & Rossman, 2016). I used interviews to collect data. Participants should feel safe and comfortable in the interview setting (Anderson, 2017). I conducted interviews in a quiet setting, such as a private room at the local library, the participant’s location, or via Skype. I ensured confidentiality by interviewing the participants with no other individuals present in the room.

Ethical Research

After gaining IRB approval, researchers must gain informed consent from the participants (Leedy et al., 2019; Lentz, Kennett, Perlmutter, & Forrest, 2016; Yin, 2018). Researchers are obligated, by law, to provide human subjects with information concerning the study unless the research is exempt from 45 CFR 46.101(b) (Miracle, 2016; U.S. Department of Health & Human Services, 1979a). The participants must have adequate time to consent and be legally competent to consent unless the guardian or legal caregiver has permitted the participant to participate in the study (U.S. Department of Health & Human Services, 1979a).

When seeking informed consent, researchers must provide participants with a declaration that participation is voluntary (U.S. Department of Health & Human Services, 1979a). Participants who refused to participate did not experience a penalty or loss of benefits. I provided the participants with adequate time to review the consent form; participants received the consent form no less than one week before the scheduled interview via email or U.S. postal service. During the scheduled interviews, I ensured that I obtained a signed copy of the informed consent form or an email that represented the consent of the participant before conducting the interview.

Researchers must plan for the possibility that participants will withdraw from research (Leedy et al., 2019; U.S. Department of Health & Human Services, 1979a; Yin, 2018). Participants who are given an option to withdraw from a study are more likely to participate and be interested in completing the interview (Yin, 2018). Participants had the right to withdraw from the study at any time. I used the withdrawal form to explain the participant's voluntary participation (see Appendix C). The participants could have informed me either verbally or in writing of their desire to withdraw via email, letter, or phone. If the participant had withdrawn from the study, I would have included information gathered from the participant before the withdrawal.

Some researchers use incentives to recruit participants for a study (Abshire et al., 2017; Annas, 2017). Researchers know little information about the regulatory guidelines for payment during the research (Abshire et al., 2017). While incentives may increase participation, incentives are not a necessity to collect information from participants (Abshire et al., 2017). Some Institutional Review Board (IRB) members are concerned that providing participants with incentives could cause coercion, thereby influencing the voluntariness of consent from the participants (Abshire et al., 2017). I did not provide incentives to participants to alleviate the possibility of coercion.

Researchers should review risk-benefit to determine the appropriateness of research involving human subjects (Leedy et al., 2019; U.S. Department of Health & Human Services, 1979b; Yin, 2018). There are three basic ethical principles relevant to ethical research: (a) respect of persons, (b) beneficence, and (c) justice (U.S. Department of Health & Human Services, 1979b). Applying respect of person to research requires the researcher to respect individuals as autonomous agents and protect those who are not capable of being autonomous (U.S. Department of Health & Human Services, 1979b). Beneficence is respecting the participant's decisions and welfare (U.S. Department of Health & Human Services, 1979b). Justice is to treat equal individuals equally (U.S. Department of Health & Human Services, 1979b). To ensure the protection of the participants, I adhered to the ethical standards suggested by the Belmont Report and Walden University's IRB.

Researchers should share their method of protecting the participants and the data (Leedy et al., 2019; Yin, 2018). To enhance the security and confidentiality of the data, I encrypted all electronic devices. I stored all the physical data in my home in a locked filing cabinet. As required by the university, I will keep all information for 5 years; after 5 years, I will destroy the data by using a paper shredder and KillDisk software. KillDisk software will allow me to dispose of information on electronic devices properly.

Researchers ensure the participants' confidentiality by protecting the identity of the participants (Lancaster, 2017; Uneke, Sombie, Lokossou, Johnson, & Ongolo-Zogo, 2017). I used pseudonyms to protect the identity of the participants. For example, I identified Participant 1 as P1 and so forth. Qualitative researchers may conceal the identity of participants with pseudonyms (Allen & Wiles, 2016). I also used the same pseudonym to identify the transcribed documentation of the associated participant. Researchers should include statements in the consent form assuring participants that their occupation, characteristics, background, and the city are confidential (Greenwood, 2016).

Data Collection Instruments

Data collection is the process in which researchers perform a course of events to gather information to answer the research question (Fusch & Ness, 2015; Van den Berg & Struwig, 2017). In qualitative studies, the primary research instrument in data collection is the researcher (Yin, 2018). In this study, I served as the primary instrument during data collection.

Interviews are a sufficient method for data collection (Awiagah, Kang, & Lim, 2016). I used semistructured interviews. Semistructured interviews are an adequate qualitative data collection technique that creates structure during interviews to allow the researcher to remain focused (Yin, 2018). I used semistructured interviews with open-ended questions to gain insight into the strategies needed by small business owners to reduce data security breaches. A researcher should develop interview questions designed to elicit answers to the research question (Pomare & Berry, 2016). Semistructured interviews are in-depth interviews designed for participants to provide answers to preset open-ended questions (Jamshed, 2014). Researchers use semistructured interviews to conduct interviews with individuals or focus groups for 30 minutes to an hour (Jamshed, 2014). When little information exists about a topic, semistructured interviews are useful when researching a phenomenon (Robinson, Ford, & Goodman, 2018). By conducting semistructured interviews, I increased the chances of reaching data saturation.

Using open-ended questions allow participants to share in-depth details on the topic and promote problem-solving strategies (Levitt, Pomerville, Surace, & Grabowski, 2017). Qualitative researchers use open-ended questions to provide participants with the opportunity to share their ideas and thoughts without limitations (Ip et al., 2016; Levitt et al., 2017). As a qualitative researcher, I encouraged participants to share their perceptions and experiences as an effort to collect extensive data. I asked probing open-ended questions while actively listening and recording participants.

Researchers should follow an interview protocol to enhance the accuracy of the information captured during the interview (Mwangi et al., 2017; Yin, 2018). The interview protocol consisted of the following steps (a) set up recording equipment, (b) introduce myself to the participant, (c) briefly describe my role relating to the study, (d) discuss the purpose of the study, (e) obtain signed consent, and (f) get permission to record the interview session. I asked seven interview questions. The duration of the interviews were 45 to 60 minutes. To answer the research question, I developed interview questions based on the overarching research question.

Member checking is the process in which the participants verify the accuracy of the information collected during the interview (Liao & Hitchcock, 2018). Using member checking allows participants to correct errors and challenge the researcher’s interpretation of the data (Birt et al., 2016; Patton, 2015). After I transcribed the audio recordings, I provided a copy of my interpretations of participants’ answers to interview questions and ask participants to verify the accuracy of my interpretations.

Reviewing organizational documents increases validity in qualitative studies (Olivier, 2017; Yin, 2018). Researchers using case studies should include company handbooks and annual reports to improve data reliability (Harrison, Banks, Pollack, O’Boyle, & Short, 2017). I requested company documentation, such as company handbooks and data security policies and procedures, from the participants who chose to participate in the study.

Data Collection Technique

Heath, Williamson, Williams, and Harcourt (2018) found that providing participants with a choice to conduct interviews using multiple methods such as Skype or face-to-face may improve recruitment and response rate. AlKhateeb (2018) argued that the advantages encountered during the data collection process when using Skype and face-to-face outweighed the limitations discussed in the literature. To increase recruitment in this study, I provided participants with the option to conduct the interviews by either using Skype or conducting face-to-face interviews.

I used semistructured interviews with open-ended questions as a data collection technique. Using semistructured interviews allow researchers to collect rich and descriptive data about the participants’ experiences (Marshall & Rossman, 2016). The interview consisted of a minimum of four small business owners. The small business owners answered seven interview questions during the interview. I delivered invitations via U.S. postal service or email.

Qualitative researchers typically conduct interviews one at a time in an isolated location (Dawson, Hartwig, Brimbal, & Denisenkov, 2017; Heath et al., 2018). I interviewed each participant individually in a private location. I provided the participants with the option to interview at the local library, in a private room, or at their business location in a private room or by Skype. If the participants had chosen to meet at the local library, I would have reserved a private room after receiving consent. The advantages of in-depth interviews are (a) collecting rich data and detail, (b) exploring the topic in-depth, and (c) using member checking (Li et al., 2015; Yin, 2018). The disadvantages of in-depth interviews are experiencing time-constraints and interviewee misrepresentation (Yin, 2018). To reduce time-constraints and interview misrepresentation, I set a timeframe of 45 to 60 minutes for interviews and added member checking.

A researcher should use processes to ensure that the interpretations of the participant's experience are accurate (Rowley, 2016). With the permission of the participants, I audio recorded the interviews. Interviews and data recording devices are a means to collect data from the participants (Leedy et al., 2019; Li et al., 2015; Yin, 2018). The typical approach to review interviews is to analyze audio recordings (Greenwood, Kendrick, Davies, & Gill, 2017). I recorded the participants to increase the accuracy of the interviews. I used an Olympus digital recorder to record interviews. The recorder allowed me to transfer files between the recorder and my computer. The device had a noise-canceling microphone for playback clarity with 4GB of built-in memory. The storage in the Olympus stores up to 1,570 hours. Researchers save and collect data during the data collection phase using more than one storage technique (Leedy et al., 2019; Yin, 2018). I also saved the transcribed information to a jump drive.

Researchers use digital recording devices because of ease of use, clarity, and increased storage (Annink, 2017). Qualitative researchers rarely used cellular devices (Garcia, Welford, & Smith, 2016). Apps on cellular devices could be unreliable software (Garcia et al., 2016). Symantec researchers conducted a study on mobile apps and found that out of 6 million mobile apps, 15% contained vulnerabilities (Alsaleh, Alomar, & Alarifi, 2017). I used a digital recorder as oppose to a cellular device to reduce the risk of comprising the participants' private responses. Cellular devices pose security risks (Alsaleh et al., 2017). Cellular device vulnerabilities increased by 32% from 2014 to 2015 (Alsaleh et al., 2017). The advantages of using electronic forms of data collection are (a) ease in managing data electronically for editing and analysis, (b) ease to facilitate, and (c) ease to automate data comparison (Li et al., 2015). Disadvantages of using electronic forms of data are (a) lack of familiarity with software packages, (b) changes to software versions, and (c) difficulty managing documents, and (d) security risk (Alsaleh et al., 2017; Li et al., 2015). To manage the disadvantages of using an electronic data collection method, I familiarized myself with the device and any associated software.

I used member checking for data interpretation in the study. I contacted participants within one week after the interview to provide them with my interpretation of their responses to the interview questions. I asked them to verify the accuracy of my interpretations. Participants had one day to review responses and provide feedback via phone or email. Member checking is a process that consists of reviewing a researcher's interpretation of participants’ answers to validate and verify the data collected (Birt et al., 2016; Leedy et al., 2019; Patton, 2015). Utilizing member checking will increase the truthfulness and accuracy of the data collected (Patton, 2015). Member checking also allows the participant the opportunity to share additional information related to the study (Patton, 2015). I did not use a pilot study for the study. Qualitative researchers use member checking, documentation, and audio recordings for data collection (Liao & Hitchcock, 2018). I searched the websites of the selected companies for the employee handbooks and data security policies and procedures, and I requested the information from the participants.

Researchers use secondary data to increase reliability and validity (Harrison et al., 2017; Olivier, 2017; Yin, 2018). Combining secondary data with interviews create triangulation to gain insight into a phenomenon (Johnson et al., 2017). I used methodological triangulation to increase my understanding of the phenomenon. Methodological triangulation is an appropriate form of triangulation in qualitative studies (Cuervo-Cazurra, Andersson, Brannen, Nielsen, & Rebecca Reuber, 2016). Triangulation increases the opportunity for a researcher to reach data saturation (Fusch & Ness, 2015).

Researchers should review the documentation for relevance and determine if the information will contribute to answering the research question and fit the conceptual framework of the study (Ridder, 2017). Documentation includes brochures, organizational and institutional reports, and public records (Hense & McFerran, 2016). There are advantages and disadvantages of using secondary documentation in research. Advantages in using secondary documentation include (a) less time consuming, (b) nonreactive to the research process, and (c) broad coverage of information (Watts et al., 2017). Disadvantages in using secondary documentation include (a) developing bias selectivity, (b) difficulty retrieving information, and (c) producing information for a purpose other than research (Watts et al., 2017). The advantages of adding documentation as secondary data to research studies outweigh the disadvantages of including secondary data (Watts et al., 2017).

Data Organization Technique

Researchers use computer software for complex qualitative research (e.g., Zotero, NVivo) to organize notes, annotated bibliographies, and other research data (Leedy et al., 2019; Woods, Paulus, Atkins, & Macklin, 2016; Yin, 2018). Data organization increases the integrity of transcribed data (Yin, 2018). For transcribing and coding, I uploaded all data collected during the interviews to NVivo 12. Qualitative researchers have a plethora of CAQDAS software to perform data analysis, such as ATLAS.ti, MAXQDA, and NVivo (Carmichael & Cunningham, 2017; Chandra & Shang, 2017; Woods et al., 2016).

NVivo has many of the same features as ATLAS.ti and MAXQDA. NVivo is a data analysis tool that improves and enhances data research with idea management, data query, reporting, data management, and graphical modeling (Damani et al., 2018). Unlike ATLAS.ti and MAXQDA, NVivo supports more data formats such as PDF’s, audio files, pictures, excel, and word (Ruggunan, 2016). I chose NVivo 12 in place of ATLAS.ti because of the ability to better process data internal or external to the project database. MAXQDA does not allow researchers to process files after the file becomes a project

(Ruggunan, 2016). I did not choose MAXQDA as opposed to NVivo 12 because of cost and file constraints.

After I loaded the raw data into NVivo 12, I searched for themes in the data. Grouping techniques will assist in identifying themes in the data (Fusch & Ness, 2015). Qualitative researchers use a coding technique to protect the participants' identities (Barnhill & Barnhill, 2015; Leedy et al., 2019; Yin, 2018). To protect the confidentiality of the participants, I removed names and addresses and implemented a coding process using letters and numbers. All physical data should be stored in a locked filing cabinet to protect the confidentiality of the participants (Rumbold & Pierscionek, 2017). I stored all the data in a locked filing cabinet in my home. No other individuals have access to the data. After 5 years, I will destroy physical documents with a paper shredder and destroy electronic data with KillDisk software.

Data Analysis

Data analysis in qualitative research is a process of techniques used to evaluate data. Researchers observe the data in search of patterns using a coding technique (Leedy et al., 2019; Yin, 2018). A case study researcher often initiates the data analysis phase during the data collection process.

The use of triangulation in the study increased reliability. Triangulation is the use of multiple sources of data (Mauceri, 2016; Olivier, 2017). Secondary data increases the richness and depth of the data (Mauceri, 2016; Olivier, 2017). I used company handbooks, data security policies, and procedures as secondary data when the information was available. Qualitative researchers use triangulation to improve the validity of the research questions (Mauceri, 2016; Olivier, 2017).

Yin (2018) introduced five steps to analyze qualitative data: (a) compiling, (b) disassembling, (c) reassembling, (d) interpretation, and (e) conclusion. To analyze the data in the study, I applied Yin’s five step data analysis. Compiling is Phase 1; to compile the data requires the researcher to sort field notes and information collected from other data resources (Yin, 2018). Disassembling is the second phase; to disassemble the data consists of breaking the original compiled data into smaller groups (Yin, 2018).

Phase 3 is reassembling; the researcher reassembles the data from Phase 2 into emerging themes (Yin, 2018). Researchers use computer-based software to reassemble the data. Interpretation is Phase 4; this phase is the researcher’s interpretation of the reassembled data (Yin, 2018). Interpretation may cause the researcher to disassemble the data or reassemble the data in a different way (Yin, 2018). Phase 5 is the conclusion; the researcher concludes the entire study based on the interpretation of the data in the fourth phase (Yin, 2018). The five stages are an iterative and reoccurring process of assembling and reassembling data (Yin, 2018).

The researcher should also search for alternate data sources using triangulation (Johnson et al., 2017; Leedy et al., 2019; Yin, 2018). Researchers use triangulation as a validity strategy in qualitative research (Korstjens & Moser, 2018). I used methodological triangulation. Within method and across method are two types of methodological triangulation (Sykes, Verma, & Hancock, 2018). *Across method* requires the researcher to combine qualitative and quantitative data collection techniques, while *within methods* allows the researcher to use observations and interviews (Sykes et al., 2018). To support data analysis in the study, I used the *within* method by conducting interviews and reviewing company documentation. Researchers use methodological triangulation to improve the validity of findings and provide conclusive data (Olivier, 2017; Sykes et al., 2018).

Researchers use documentation analysis in conjunction with other qualitative data collection methods to display corroboration (Johnson et al., 2017). Applying the different data collection techniques increased the opportunity to identify similarities and discrepancies in the data. I used the comparative method. The comparative method includes (a) grouping comparable themes into larger groups, (b) comparing emerging themes, and (c) reporting findings (Shams, Sari, & Yazdani, 2016; Yin, 2018). I grouped data according to the themes that emerged from the data collected by using NVivo 12; software developed to organize and analyze data.

NVivo handles most data, including notes, Word documents, PDFs, spreadsheets, and audio files. NVivo is a computer assisting qualitative data analysis tool (CAQDA). CAQDA is helpful for coding data (Yin, 2018). Using NVivo 12, I was able to upload my transcripts and secondary data for the analysis phase. Pattern-based auto coding methods within NVivo 12 allowed me to code large volumes of text quickly. I developed themes before and during the interview process using NVivo 12 as coding software. Coding consists of reviewing the data and looking for distinct concepts and themes in the data (Yin, 2018). Qualitative researchers should analyze data from all angles (Abdalla et al., 2018). My first step in the coding process was to review the literature for original patterns and track this information in NVivo 12.

Researchers use data analysis to identify information and themes that are relevant to the central research question (Leedy et al., 2019). Researchers who correlate the findings of research with the principles of the conceptual framework and current literature increase validity and structure for the methodology (Bogers et al., 2017). I correlated the findings of my study with my conceptual framework and current research. I interviewed the participants until no new themes developed. I loaded the information into NVivo 12 and used nodes to create codes. Researchers use nodes in CAQDA software to identify themes and codes in research data (Yin, 2018).

Reliability and Validity

Reliability

Reliability is the consistency of findings (Aravamudhan & Krishnaveni, 2016). A reliable instrument can produce the same results when repeated with the same basic concept (Aravamudhan & Krishnaveni, 2016; Leedy et al., 2019; Yin, 2018). To establish reliability in the study, I provided instructions and develop clear and concise interview questions. Clear and concise interview questions increase reliability (Amankwaa, 2016; Merriam & Tisdell, 2016; Yin, 2018). I requested the participants to use member checking to review the transcribed interview. Researchers use member checking to increase reliability (Birt et al., 2016; Connelly, 2016; Patton, 2015). A comparison of transcribed interviews and recordings increased the accuracy of the data.

Dependability in qualitative research improves with consistency in the research data collection process (Yin, 2018). When the research techniques are repeatable and replicable, dependability is enhanced (Iivari, 2018; Yin, 2018). Colleagues in the field verifying data interpretation (Iivari, 2018; Leedy et al., 2019) may also establish dependability.

Validity

To improve the quality of qualitative research, researchers should reveal their assumptions and values (Ridder, 2017). Revealing assumptions and values demonstrates the views of the researcher and exposes biases (Rau, 2020; Yin, 2018). I reduced the bias input by revealing my connection to the study. Establishing instruments and procedures ensure the validity and authenticity of the research findings and results (Nico, 2016). An instrument is reliable when participants have clear and concise interview questions (Van den Berg & Struwig, 2017). I was the primary instrument in the study. Participants received a sample of the interview questions in advance to improve my chances of collecting more reliable data. I distributed the sample interview questions no less than one week via email or by U.S. postal services.

Credibility is the process of participants confirming the accuracy of the interpretation and representation of the data presented by the researcher (Keikha, Hoveida, & Nour, 2017). Participants create credibility through member checking (Iivari, 2018). Member checking occurs when the participants review the findings of a study (Birt et al., 2016; Connelly, 2016; Iivari, 2018). I used member checking to increase validity and review the results of my findings. Participants reviewed my interpretations of their answers to ensure that I accurately captured the responses during the interview.

Researchers should share their experience as a researcher and verify the findings with the participants to display credibility (Liao & Hitchcock, 2018). To increase qualitative credibility, researchers should demonstrate thorough engagement observation and notetaking (Liao & Hitchcock, 2018). I shared my experiences and findings with the participants to display my credibility.

Researchers establish transferability when readers and participants can relate a study to their circumstances (Parker & Northcott, 2016). Researchers improve transferability by ensuring applicability to the culture and characteristics of the participants (Iivari, 2018; Moon, Brewer, Januchowski-Hartley, Adams, & Blackman, 2016). Researchers using transferability can also assist with judging the research findings by providing an outline of how they identified and chose the participants (Moon et al., 2016). I established transferability in the study by sharing my findings after the study was completed, approved, and submitted to ProQuest. Publishing the study will provide future researchers with the opportunity to transfer the findings to other participants and settings.

Confirmability meets the requirements in qualitative research to display the truthfulness of the data. Confirmability is the result of the experiences and perceptions provided to the researcher by the participants (Abdalla et al., 2018). Developing additional individuals or methods besides the researcher involved in the data analysis stage allows the researcher to confirm and verify findings (Park & Park, 2016). I ensured confirmability in the study by using triangulation.

Researchers reach data saturation when no new themes emerge during the data collection process (Marshall & Rossman, 2016). When researchers find redundancy and repetition in the data, they have achieved data saturation (Boddy, 2016; Hammarberg, Kirkman, & de Lacey, 2016; Jin et al., 2018). I used purposeful sampling. I also interviewed participants until redundancy and repetition were present in the data. Data saturation is essential in qualitative research to ensure validity, confirmability, credibility, and transferability (Carmichael & Cunningham, 2017).

Transition and Summary

Section 2 contained a detailed description of the role of the researcher, participants, research method, research design, population and sampling, ethical research, data collection, data organization, data analysis, and reliability and validity. Section 3 contains an introduction, presentation of the findings, application to professional practice, and a more detailed explanation of the implications for social change. Recommendations for actions and recommendations for further studies are in Section 3, as they relate to the topics within the study that need a more in-depth investigation and may produce additional questions to improve practice in business. Section 3 also includes my reflections on my experience during the research process in which I discuss any bias or predetermined thoughts and values. I complete Section 3 with a concluding statement.

Section 3: Application to Professional Practice and Implications for Change

Introduction

The purpose of this qualitative multiple case study was to explore strategies small business owners use to reduce data security breaches. The data came from small business owners and company documentation at four small businesses located in the southern region of the United States. The study may contribute to positive social change by rebuilding the relationships between business leaders and consumers. Rebuilding relationships between business leaders and consumers could result in increased spending to support local communities and improve the financial health of the local economy (Nguyen et al., 2015). In this study, I discovered the security methods small business owners used to reduce data security breaches.

Presentation of the Findings

The overarching research question for the study was as follows: What strategies do small business owners use to reduce data security breaches? Organizations affected by data security breaches may experience reputational damage and remediation costs (Gwebu et al., 2018). Tadesse and Murthy (2018) reported that small business owners experienced 71% of all data security breaches. It is pertinent to protect a system from unauthorized access and disruptions to minimize data security breaches (Horne et al., 2017). In this study, I selected four small business owners. The participants shared the methods used to secure their data. The participants varied by business type, years of experience, and demographics.

Demographics

Demographics add additional insight into the characteristics of the participants. Participants' demographics could impact their decision making on the adoption of specific technologies (Rojas-Mendez, Parasuraman, & Papadopoulos, 2017) and the strategies used to protect their organizations (Wang, Xu, Li, & Chen, 2018). Describing the demographics of the participants could also increase the validity and replication of the findings.

The participants were selected using a purposeful sample. The business types included a travel agent, funeral home director, insurance agent, and a restaurant owner. The selected business owners have been in business for more than 5 years. I concealed the identity of the participants using a pseudonym name.

P1 was a franchise small business owner with 15 years of experience as a travel agent. P1 did not own a storefront for business operations. P1 stated that P1 conducted 100% of the business online. No financial transactions took place through the company's website. All clients were required to contact P1 by phone to complete financial transactions.

P2 was a nonfranchise small business owner with 9 years of experience as a funeral home director. The small business owner had a website used to illustrate the services offered by the organization. However, while P2 had a website, all business and financial transactions with clients took place face-to-face at the funeral home.

P3 was a franchise small business owner with 34 years of experience in the insurance industry. P3 conducted business using storefront and online services. Clients could make financial transactions in the office or online.

P4 was a nonfranchise small business owner with 9 years of experience as a restaurant owner. P4 did not have an online website to conduct business. All customer orders and financial transactions took place in the restaurant.

The demographics of participants were shared to describe my sample accurately. Future researchers will have the ability to replicate this study by having demographic information. Describing the demographics provided a more in-depth understanding of the similarities and differences found in the responses during the data analysis. Table 1 is a depiction of the demographics of the participants in this study.

Table 1

Demographics

Category	P1	P2	P3	P4
Gender	Male	Male	Female	Female
Business Type	Travel Agent	Funeral Home Director	Insurance Agent	Restaurant Owner
Years of Service	15	9	34	9
Franchise/ Nonfranchise	Franchise	Nonfranchise	Franchise	Nonfranchise

I used NVivo 12 qualitative data management system to assist me in discovering new insights and trends. I imported eleven documents, including four participant interviews and seven organizational documents, which I used to code and analyze the data. I discovered seven themes using NVivo's auto-coding feature. I narrowed the list down to two themes. Large amounts of text data were added using the NCapture feature to import web and social media content. I created nodes by auto-coding each sentence. Two major themes emerged from the data. The themes aligned with the research question and the conceptual framework. The themes that emerged are (a) information assurance (b), and third-party dependency, as presented in Table 2.

Table 2

List of Major Themes

Themes	Sources	References
Information Assurance	12	1394
Third-party Dependency	11	482

Theme 1: Information Assurance

Information assurance was the first theme that I used to reveal insight into the strategies small business owners use to reduce data security breaches. Information assurance is a set of security strategies that protect the confidentiality, authentication, integrity, and availability of the data (U.S. Department of Commerce, 2017b). These measures include providing for restoration of information systems in case of data loss (Nieles, Dempsey, & Pillitteri, 2017).

I analyzed the organizations' documentation and participants' interview responses and, as a result, the theme information assurance emerged from the data. All participants acknowledged information assurance, as a strategy, small business owners use to reduce data security breaches. Using a text query, Table 3 includes a thematic synthesis of the importance of information assurance, as expressed by the participants.

Table 3

References and Frequencies of Information Assurance

Source	Reference	Frequency (%)
P1, Interview /Organizational Documentation	681	26.55
P2, Interview/ Organizational Documentation	264	28.67
P3, Interview/ Organizational Documentation	399	48.94
P4, Interview/ Organizational Documentation	50	14.12

Business owners can use data to make decisions for the operation and success of businesses (Horne et al., 2017; Kauspadiene, Ramanauskaite, & Cenys, 2019). Employing strategies to protect the confidentiality, integrity, and availability of the data is needed to ensure trust with customers and the protection of sensitive data (Horne et al., 2017). There is not a specific set of security strategies that all businesses should use for data protection (Burdon & Coles-Kemp, 2019; Ming, Chen, & Guo, 2019). Using multiple methods could decrease the chances of a company experiencing a data security breach (Ming et al., 2019). The participants provided their existing strategies used to protect their data. The strategies varied between the participants and consisted of password protection, encryption, and data recovery.

Passwords are still relevant to secure a system (Kaleta, Lee, & Yoo, 2019). Users should create strong passwords. Weak passwords leave the system vulnerable (Kaleta et al., 2019). Users' inability to remember passwords may cause them to create weak passwords (Kaleta et al., 2019). Creating user-IDs with strong passwords decreases the likelihood of illegal access (Kaleta et al., 2019).

P1, P2, and P3 developed websites that require users to create a user-ID and password to obtain access to the system. In addition to requiring users to create a user-ID and password to access the system, P1, P2, and P3 also require employees to use a username and password to access the organizations' system. During member checking, I asked P4 if P4's business computer was password protected. P4 stated that the computer was password protected and that only P4 and P4's espouses had access to the computer.

The requirements implemented by P1, P2, P3, and P4 align with current literature. Security experts suggest that passwords are a secure method to prevent unwanted access (Kaleta et al., 2019). Only P2 required employees to change their passwords frequently, every three to six months. Security experts also recommend that business owners should implement policies and procedures requiring users to amend their passwords every 90 days or less (Yu et al., 2017).

P2 stated, "the employees are provided with a unique user-ID and password to easily identify who is accessing and making changes to the system." Similar to P2, P3 stated, "each employee is provided with a four-digit user-ID that is unique to each employee." P3 used the user-ID to see who made changes to the system. P3 also stated, "we have password rules in the office; no one can use the other person's password."

P3 was the only participant mentioning a form of two-factor authentication as an additional method to protect data. P3 stated that the employees used a security token in addition to their passwords to access information. The security token was a second method used to identify a user in the system, also known as two-factor authentication.

Two-factor authentication strengthens password protection (Esiner & Datta, 2019). Users are required to employ two forms of identification when using two-factor identification (Esiner & Datta, 2019). Two-factor authentication increases security by using a secondary method when identifying a user (Esiner & Datta, 2019). Business leaders use encryption methods to ensure confidentiality, integrity, authentication, and nonrepudiation (Chen, Lopez, Martinez, & Castilleio, 2018; Shi & Guan, 2019).

In addition to passwords, some of the participants used services that contained encryption methods, such as a secure socket layer (SSL). An SSL was used to decrypt messages sent over the network (e.g., Internet, email, browser) and authenticate the user conducting the action (Chen et al., 2018; Owoh & Mahinderjit Singh, 2018). User information, such as credit card and login information, are confidential and protected from hackers when transmitted using SSL encryption (Morris, Rogaway, & Stegers, 2018).

The participants consisted companies. P1 stated, “the corporation backup our data using 128 encryptions of two franchise and two nonfranchise. This encryption is part of the highest standards of encryption.” P2 purchased third-party services that encrypt the system using SSL. In P2’s third-party security policy, SSL was the security method used to protect the organization’s data. The third-party privacy policy stated, “we use encryption to keep your data private while in transit. Setting your site up with an SSL certificate to provide HTTPS protection is a fundamental step for securing your website.”

P3’s privacy policy stated that financial transactions are confidential. According to the information in the private policy of the corporate office, the system was encrypted “using the most recent release of SSL technology with encryption keys of up to 128 bits”.

P4 transmits the company’s financial data through a bank. The policies stated, “we require the use of a 128-bit encryption secure browser before a connection can be made to the transaction system”. P4 also transmitted customer credit card data using a credit card machine. P4 stated,

> We do have a credit card machine. We handle most of the transactions. However, we do have employees that have to swipe credit card information. We keep an eye on them and make sure that they are not copying credit card information or taking pictures of the credit card information.

Credit card payments can create data security vulnerabilities for small business owners (Clapper & Richmond, 2016). Small business owners should implement strategies to reduce illegal access (Karanja & Rosso, 2017). Hackers also use point of sales to gain access to private data in more substantial corporations (Karanja & Rosso, 2017). P4’s strategy to monitor employees to keep them from copying credit card information and taking pictures does not align with the literature.

Dishonest employees having access to cash registers pose a threat to data security (Frazer, 2016). As recommended by the Payment Card Industry Data Security Standard, all businesses that use a credit card as the point of sale for payment transactions are encouraged to have automatic antivirus software, regular self-assessment, security plan, and network evaluation (Clapper & Richmond, 2016).

Information assurance also includes adding a method to recover data during a breach or system failure, such as contingency planning. A contingency plan is a response plan to mitigate the loss of services (Nieles et al., 2017). Contingency planning allows business leaders to respond quickly in the event they experience a disruption in operation (Nieles et al., 2017). Business leaders should develop a contingency plan for the system to determine the way the system obtains the outage as well as a method to recover the data (Nieles et al., 2017). The plan should also contain information on how to continue operations in the case of a security breach or natural disaster (Nieles et al., 2017).

Rossmiller, Lawrence, Clouse, and Looney (2017) stated that small business owners fail to implement a technical contingency plan because technology is not considered a high priority for small business owners. The findings from this study support the claims found in Rossmiller's research on disaster recovery plans in small businesses. Fifty percent of the participants did not see the importance of having a contingency plan. I asked the participants what they would do if an actual breach occurred internally or externally. I only received a contingency plan from P3 and P4. P1 and P2 stated that because they have not had a breach, there has not been a need to be concerned about developing a contingency plan. The contingency plans offered by P3 and P4 were not complete. The plan from P3 only included actions if the organization experienced an internal threat. P4 included a plan for an internal and external threat.

During member checking, P3 stated, "if we experience a security breach, all of our data is backed up by the corporate office." P4 said,

> If a breach occurred internally, we would check our security cameras to see if any of our employees were involved. If a breach occurred externally, we use prepaid legal to help us with external issues. So, if anything occurred, we would mitigate those issues directly with our bank. They should have their process for dealing with external data security breaches.

P4 provided me with the name of the financial institution used to support the business. I reviewed the privacy policies from the bank's company website. The security practices used by the bank owners included encryption, firewalls, and user-ID and passwords to protect consumers' data.

Theme 1, information assurance, aligns with systems theory. Systems theory consists of interconnected parts. Information assurance is part of the process to secure organizational information within the system. Information assurance is a set of interrelated security strategies that protect the confidentiality, integrity, and availability of the data (U.S. Department of Commerce, 2017b). Applying strategies to protect the data is a series of procedures (input) that work together to produce a positive or negative outcome (output). Knowing the inputs, outputs, and the environment increases the performance of business organizations (Hester, 2014).

Systems theory is relevant to review the data security strategies used by small business owners to reduce data security breaches. Systems theory is about interrelated parts and relationships of a system that interact in its entirety and not in separate parts (Bertalanffy, 1968). Systems theory provides a theoretical basis to examine all systems within an organization. An organization is a system with subsystems (Yadav, Nepal, Rahaman, & Lal, 2017). Security processes are subsystems within an organization (Yadav et al., 2017).

Information assurance consists of processes used to protect authentication, integrity, confidentiality, availability, nonrepudiation, and recovery of the data (Nieles et al., 2017; U.S. Department of Commerce, 2017b). Figure 1 is an illustration of how Theme 1, information assurance, aligns with systems theory.

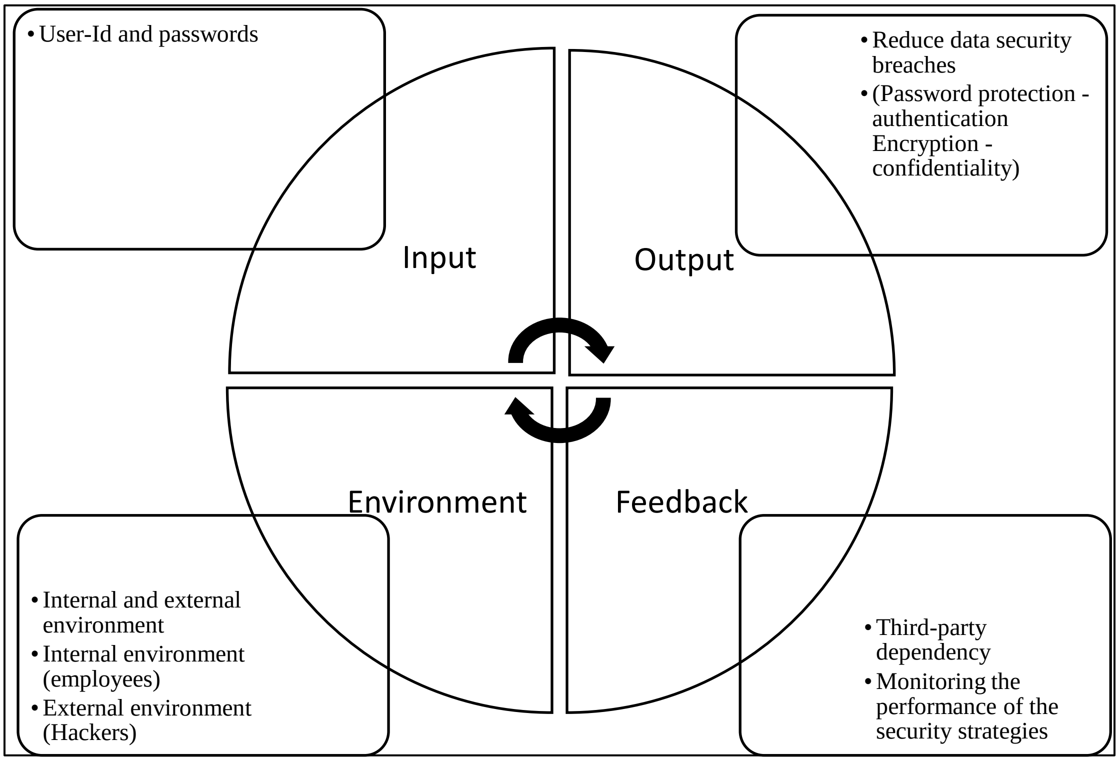
• User-Id and passwords
• Reduce data security breaches
• (Password protection - authentication Encryption - confidentiality)
Input
Output
Environment
Feedback
• Internal and external environment
• Internal environment (employees)
• External environment (Hackers)
• Third-party dependency
• Monitoring the performance of the security strategies

Figure 1. *How systems theory aligns with the information assurance.*

Authentication is verified when the users of the system provide information, such as passwords or tokens, to authenticate their access (Yuan et al., 2017). Applying strategies to protect the data consists of using controls that work together to produce a positive or negative outcome. Inputs are resources that go into the systems that are created based on the need (Sardone, 2017). The input is then processed based on the steps that lead to the output (Sardone, 2017).

The output of the authentication process determines if the user is authorized to use the system (Kauspadiene et al., 2019), which provides a method to determine the integrity, confidentiality, and nonrepudiation of the data (Kauspadiene et al., 2019). The output process includes the availability of the data. Data in the availability stage are pre-existing data that have been stored and are available to be retrieved. The availability of the data ensures that users can access the data when needed. Information should remain unavailable to users if they are not authorized to access the system (Sadiku, Alam, & Musa, 2017). Business owners can grant permission to the system through an authentication process (Sadiku et al., 2017). The authentication process provides a method to determine the availability, nonrepudiation, integrity, confidentiality, and the recovery of the data (Kauspadiene et al., 2019).

Security officers uphold confidentiality and integrity by implementing monitoring feedback techniques (Artur, 2018). Small business owners can apply monitoring methods to determine if the strategies put in place are positive or negative influences on the system. To determine if the decisions are appropriate, there must be a feedback mechanism to determine if the decisions are appropriate (Sardone, 2017; Zauwiyah, Thian, Tze, & Mariati, 2019). Business owners use feedback to control the system. The controls are created based on the experiences of the environment (Roxas, Rivera, & Gutierrez, 2019).

Business leaders recover the data using a backup method. Data backups are also digital libraries that house sensitive information that can be easily retrieved in case of data loss or breach (Singh, 2019). Business leaders should choose data backup methods based on security and business needs (U.S. Department of Homeland Security, 2016).

The environment influences the need for controls. Employees influence the environment internally while hackers influence the environment externally. Small business owners may experience a breach internally or externally. Knowing the input, output, feedback, and the environment increases the performance of business organizations (Hester, 2014).

During the data analysis, I found that participants were aware of the security challenges within their organizations, and they mitigated their issues by requiring employees and customers to use user-ids and passwords. While technology has advanced password rules and encryption methods are still highly recommended as a means of protection (Kaleta et al., 2019), only 50% of the participants had a contingency plan. Failure to implement a contingency plan can be costly for small business owners (U.S. Department of Homeland Security, 2018b).

Theme 2: Third-party Dependency

Third-party dependency is a theme referenced by all participants (P1, P2, P3, P4) as a key factor to enhance the ability to reduce data security breaches. Third-party dependency emerged from the organizations’ documentation and participants’ interview responses. All participants acknowledged third-party dependency as a strategy used to reduce data security breaches. Table 4 includes a thematic synthesis of the importance of information assurance, as expressed by the participants.

Table 4

References and Frequencies of Third-party Dependency

Data Source	References	Frequency (%)
P1, Interview/ Organizational Documentation	211	11.19
P2, Interview/ Organizational Documentation	74	11.51
P3, Interview/ Organizational Documentation	173	20.87
P4, Interview/ Organizational Documentation	24	9.15

I discovered that while the participants implemented strategies to protect their local machines, the business owners relied on third-party companies for backing up sensitive data and measuring security performance. Trends in the literature support maintaining some in-house security strategies while outsourcing costlier services (Feng, Chen, Feng, Li, & Li, 2019; Wu, Fung, Feng, & Wang, 2017). Third-party data security services can be used to secure data, access content, and store data (Esiner & Datta, 2019).

P1 and P3 relied on the corporate offices for some of their data security services. P2 and P4 used third-party companies to back up their data with no affiliation with a corporate office. Business owners use data backups to stabilize the organization after experiencing a security breach (Feng, Wang, Li, & Li, 2019). The literature did not support using a third-party to backup data. Using third-party companies to store and maintain data may pose additional security threats to a business owner (Feng, Chen, et al., 2019; Subha & Jayashri, 2017).

P1 stated, “the corporation backup our data using 128 encryptions. This encryption is part of the highest standards of encryption. As an individual franchise, we do not measure performance here, but this information is tracked at the corporate level." While 128 encryptions are highly recommended by security officers, it is no longer the highest standard of encryption (Harmouch & El Kouch, 2019; Kim, Vetter, Dongarra, & Tourancheau, 2019). Advanced encryption standards have improved with 192 and 256 encryptions (Harmouch & El Kouch, 2019).

P3 stated, "information is backed up on a server by the corporate office. Our data is backed up hourly on a server." P3 also required employees not to use external devices to save company data. P3 stated, "we are not allowed to backup data on any external devices or save any information on our personal drives on our computers." The literature supports the security concerns for external devices. External devices, such as USB drives, laptops, or portable hard drives can be misplaced or stolen (U.S. Department of Homeland Security, 2019b). Portable devices are small and are easy targets for hackers (U.S. Department of Homeland Security, 2019b).

Similar to P1 and P3, P2 and P4 also used third-party companies to back up their sensitive data. P2 stated, "sensitive data is backed-up through another company. Even if our local computer crashes, we can retrieve our information from a third-party company." P4 stated, "we backup our data with another company. For example, all our tax information is backed up by a third-party company."

During data analysis, I found that the corporate offices associated with P1 and P3 both experienced a data security breach. P1 stated, "the corporation experienced a data security breach in 2015." Unlike P1, P3 was unaware that the corporate office had experienced a security breach. Online public records revealed that P3's corporate office had experienced at least two data security breaches. P1 and P3's exposure to a security breach further strengthens previous research that business owners should not use third-party companies for data security back-ups. In this research, the third-party companies for P1 and P3 posed a data security risk to the small business owners' data.

P1, P2, and P3 used third-party companies to monitor performance. Business owners use performance monitoring offered by third-party companies to detect and reduce security breaches (Feng, Wang, et al., 2019). P1 and P3 used their corporate offices to monitor their data security performance. P1 stated, "as an individual franchise, we do not measure performance here, but this information is tracked at the corporate level. P3 also stated, "data security performance is not measured at the organization. Data security performance is measured at our corporate office." Similar to P1 and P3, P2 stated, "we don't have a tool in-house to track performance. We use a third-party company to measure our performance and inform us of a security breach." P4 was the only participant that did not have a method of measuring security performance. P4 stated, "we have never experienced a data security breach. We don't measure at our level because we are so small." While the literature did not support using third-party companies for data backup, the literature does support using third-party companies to measure data security performance.

Third-party companies can provide business owners with 24/7 data monitoring. The business owners are alerted if they experience a breach (Khalili et al., 2018). Third-party security monitoring is recommended over business owners installing security applications to monitor performance (Khalili et al., 2018). The alerts are provided to the business owners to decide on what is needed if they experience a breach (Khalili et al., 2018). Measuring performance improves services for business owners with early detection and alerts (Khalili et al., 2018).

Third-party dependency aligns with systems theory through the feedback principle. Feedback provides system owners with the knowledge to adjust to the system to meet the needs of the organization's success (Sayin, 2016). Small business owners applying the tenets of systems theory could be more effective in responding to data security breaches by becoming proactive, as opposed to reactive. I found that the participants did not review any reports or record the performance of their security practices. P1 and P3 stated that their corporate office recorded performance, but they were unaware of any of the metrics that are used to assess their security practices. Reviewing the feedback principle listed under systems theory would provide small business owners with the metrics to identify the health of their data security strategies.

Applications to Professional Practice

Organizations are using technology to improve the manner in which they conduct business (Zhu, 2019). Using technology improves business operations (Ramaswamy, 2019) as well as introduces new problems for small business owners (Horne et al., 2017). Small business owners may experience a data security breach that could ultimately disrupt services or bankrupt the organization.

In my findings, I am responding to the gap that exists between small business owners and the strategies needed to protect their systems. This study may provide small business leaders with the strategies needed to reduce data security breaches. Successful small business owners have implemented the strategies identified in the findings of this study. My findings provide a basis for a data security plan for small business owners who are not protecting their systems. Applying these strategies may reduce attacks from hackers, protect company data, and improve consumer confidence. The information collected adds to the body of knowledge on ways to reduce a data security breach.

Implications for Social Change

The U.S. workforce is made up of 30.2 million small business owners (U.S. Department of Small Business Administration, 2018). Small businesses employ approximately 47.5% of the population (U.S. Department of Small Business Administration, 2018). The implications of positive social change include the potential for small business owners to develop data security strategies to protect their organizations from experiencing a data breach, which may cause consumers to rebuild trust with small business owners and increase spending. Many businesses use electronic transactions to conduct business (Curtis et al., 2018). Consumers can easily access purchases. Protecting small businesses from data security breaches can add trust with consumers and increase spending (Curtis et al., 2018). Increased spending by consumers expand the tax base, which may provide local community leaders with the financial aid to support first responders, schools, and nonprofit organizations in the local communities. Technology affects businesses' data security as well as trade opportunities with other countries (Hizam & Amin, 2019).

Recommendations for Action

The purpose of this qualitative multiple case study was to explore strategies small business owners use to reduce data security breaches. In my findings, I revealed actions that current and future small business owners could use to secure their systems. The participants used user-IDs and passwords as a means to ensure the authentication, integrity, confidentiality, and repudiation of the data.

Small business owners should also find ways to back up their data in-house, as opposed to using a third-party company. Data should be backed up on devices that are not connected to the network (FTC, 2019). To ensure protection, small business owners should encrypt external devices with strong passwords and multi-factor authentication (FTC, 2019). Small business owners electing to use a third-party company should thoroughly research the company and security methods the third-party company uses.

I would also recommend that small business owners measure their data security performance to ensure that their strategies are appropriate for their businesses. Cloud service providers offer services that monitor security, such as servers and applications performance (Halabi & Bellaiche, 2017). Small business owners should also do further research on the laws and results of data security breaches. The participants did not have a thorough answer regarding a way to respond to a data security breach. Small business owners could improve response time to a data security breach by developing a contingency plan. Improving their knowledge could cause them to expand their data security practices. Small business owners could improve their knowledge of data security practices by setting up training modules for themselves and their employees (U.S.

Department of Small Business Administration, 2019). I would also recommend that small business owners involve their employees in the development of policies and procedures.

Future researchers should consider using NVivo as an analysis tool for research. I found the NVivo tool to be user friendly. I was able to use the auto code feature and matrix coding to find themes. It was easy to transition between different types of resources in NVivo such as uploading and viewing webpages, word documents, audio files, and PDFs. I also used the tool to create tables.

I will share my findings of this study by publishing my study in academic journals and ProQuest. Students struggle to find a journal to publish their academic literature after graduation (Ahlstrom, 2017). I am also seeking research conferences, such as the *Small Business Expo,* to present my findings to small business owners.

Recommendations for Further Research

Learning the techniques to secure data in small businesses is needed for small business success (Hallova, Polakovic, Silerova, & Slocakova, 2019). My recommendations for future studies include researching the number of data security breaches between franchise small business owners and nonfranchise small business owners. According to Paulsen (2016), weak data security practices in small businesses are a direct entry into larger corporations for cyber criminals to gain illegal access into larger corporations (Paulsen, 2016). I would also recommend conducting the study in a different part of the region of the United States and with different types of small businesses.

The limitations identified in Section 1 were addressed with a mitigation plan for each limitation. To reduce time constraints, I communicated with the participants and provided them with the consent form that listed a sample of the interview questions before the interview. I concealed the identity of the participants to mitigate the possibility of participants being dishonest. I expressed that there were no right or wrong answers. I also shared my connection to the study and used member checking to reduce bias. My final limitation was the possibility that participants could withdraw from the study at any time. To mitigate the possibility of the participants withdrawing, they were able to view the criteria in the consent form and decide to participate or reject the offer to participate in the study.

Reflections

The doctoral process was challenging. However, I found the experience enlightening. Before conducting the study, I was unaware of how much small business owners depend on third-party companies to assist in storing and securing their data. Now that I have completed the study, I found that small business owners are more involved in their data security processes than I originally believed before the study. Data security is a sensitive subject for business owners. I was more successful in obtaining participants face-to-face. I was grateful to receive participants that allowed me to interview them to gain a more in-depth insight into what was needed to protect small businesses. This experience has made me more open to taking surveys and participating in studies. Now that I have experienced how challenging it is to conduct research, I will be more open to helping others.

Conclusion

The purpose of this qualitative multiple case study was to explore strategies small business owners used to reduce data security strategies. I interviewed four participants who had successfully implemented data security strategies. During the data collection phase, I conducted semistructured interviews and reviewed organizational documents. During the data analysis, two themes emerged from the data information assurance and third-party dependency. The findings of this study were used to answer the research question. The findings also aligned with the conceptual framework, which is systems theory.

Small business owners can use the findings of this study to strengthen existing data security methods or use the findings as a basis to develop a new security plan. Cyber security is ever changing, and small business leaders should revisit their plans regularly to ensure their data security strategies are still relevant. Small business owners should also increase employee awareness and monitor data security performance to ensure they have implemented the appropriate methods.

Hackers will continue to look for ways to illegally infiltrate computer systems and steal valuable organizational and customer data. Small business leaders should continue to be proactive as opposed to being reactive to data security issues. Protecting company systems can reduce security risk, improved customer confidence, and improve the health of the economy.

References

Abbas, M. W., & Ul Hassan, M. (2017). Moderating impact of environmental turbulence on business innovation and business performance. *Pakistan Journal of Commerce and Social Sciences, 11*, 576–596. Retrieved from http://www.jespk.net/

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

Abdullahi, M., Gesimba, P., & Gichuhi, D. (2017). Effects of routing and scheduling plans, logistical procedures, and customer service on delivery of courier services at the Postal Corporation of Kenya. *Journal of Strategic Management, 1*, 13–28. Retrieved from https://ajpojournals.org/journals/index.php/JSM

Abshire, M., Dinglas, V. D., Cajita, M. I. A., Eakin, M. N., Needham, D. M., & Himmelfarb, C. D. (2017). Participant retention practices in longitudinal clinical research studies with high retention rates. *BMC Medical Research Methodology*, *17*(30), 1-10. doi:10.1186/s12874-017-0310-z

Adams, K. M., Hester, P. T., Bradley, J. M., Meyers, T. J., & Keating, C. B. (2014). Systems theory as the foundation for understanding systems. *Systems Engineering, 17*, 112–123. doi:10.1002/sys.21255

Aguilar, L. (2015). *The need for greater focus on the cybersecurity challenges facing small and midsize businesses*. Retrieved from www.sec.gov/news/statement/cybersecurity-challenges-for-small-midsize-businesses.html#_edn35

Ahlstrom, D. (2017). How to publish in academic journals: Writing a strong and organized introduction section. *Journal of Eastern European & Central Asian Research, 4*(2), 1-9. doi:10.15549/jeecar.v4i2.180

Ahmed, A., Latif, R., Latif, S., Abbas, H., & Khan, F. A. (2018). Malicious insiders attack in IoT based multi-cloud e-healthcare environment: A systematic literature review. *Multimedia Tools and Applications, 77*, 21947–21965. doi:10.1007/s11042-017-5540-x

Ajzen, I., & Kruglanski, A. (2019). Reasoned action in the service of goal pursuit. *Psychological Review, 126*, 774–786. doi:10.1037/rev0000155

Al-Alawi, A. I., Al-Kandari, S. M., & Abdel-Razek, R. H. (2016). Evaluation of information systems security awareness in higher education: An empirical study of Kuwait University. *Journal of Innovation and Business Best Practice, 2016*(2016), 1–24. doi:10.5171/2016.329374

Alexander, G. L., Kiernan, M., Oppezzo, M. A., & Resnicow, K. (2018). Effects of a methodological infographic on research participants' knowledge, transparency, and trust. *Health Psychology, 37,* 782-86. doi:org/10.1037/hea0000631

AlKhateeb, M. (2018). Using Skype as a qualitative interview medium within the context of Saudi Arabia: A research note. *Qualitative Report, 23*, 2253–2260. Retrieved from https://nsuworks.nova.edu/tqr/

Allen, A., Barnard, E., Gillam, L., Guillemin, M., Rosenthal, D., Stewart, P., & Walker, H. (2018). Do research participants trust researchers or their institution? *Journal of Empirical Research on Human Research Ethics, 13,* 285-294. doi.org/10.1177/1556264618763253

Allen, J. (2014). It's two A.M.: Do you know where your data is and who can access it. *American Journal of Family Law, 28,* 20–24. Retrieved from https://lrus.wolterskluwer.com/store/product/american-journal-of-family-law/

Allen, R. E., & Wiles, J. L. (2016). A rose by any other name: Participants choosing research pseudonyms. *Qualitative Research in Psychology*, *13,* 149–165. doi:10.1080/14780887.2015.1133746

Almalki, S. (2016). Integrating quantitative and qualitative data in mixed methods research—Challenges and benefits. *Journal of Education and Learning, 5,* 288–296. doi:10.5539/jel.v5n3p288

Almaney, A. (1974). Communication and the systems theory of organization. *International Journal of Business Communication*, *12,* 35–43. doi:10.1177/002194367401200106

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

Alsaleh, M., Alomar, N., & Alarifi, A. (2017). Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods. *PloS one*, *12*(3), 1–35. doi:10.1371/journal.pone.0173284

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

American Psychological Association. (2010). *Publication manual of the American Psychological Association*. Washington, DC: American Psychological Association.

Amundsen, D. D., Msoroka, M., & Findsen, B. (2017). “It’s a case of access”: The problematics of accessing research participants. *Waikato Journal of Education, 22*(4), 5–17. doi:10.15663/wje.v22i4.425

Anderson, V. (2017). Criteria for evaluating qualitative research. *Human Resource Development Quarterly*, *28*, 125-133. doi:10.1002/hrdq.21282

Andrews, D. R., No, S., Powell, K. K., Rey, M. P., & Yigletu, A. (2016). Historically black colleges and universities’ institutional survival and sustainability: A view from the HBCU business deans’ perspective. *Journal of Black Studies, 47*, 150-168. doi:10.1177/0021934715622220

Annane, B., & Ghazali, O. (2019). Virtualization-Based Security Techniques on Mobile Cloud Computing: Research Gaps and Challenges. *International Journal of Interactive Mobile Technologies, 13*(4), 20–32. doi:org/10.3991/ijim.v13i04.10515

Annas, G. J. (2017). Informed consent: Charade or choice? *The Journal of Law, Medicine & Ethics, 45*, 10-11. doi:10.1177/1073110517703096

Annink, A. (2017). Using the research journal during qualitative data collection in a cross-cultural context. *Entrepreneurship Research Journal, 7*(1), 1-17. doi:10.1515/erj-2015-0063

Aravamudhan, N. R., & Krishnaveni, R. (2016). Establishing content validity for new performance management capacity building scale. *IUP Journal of Management Research*, *15*, 20-43. Retrieved from http://www.iupindia.in/Management_Research.asp

Arnold, R. D., & Wade, J. P. (2015). A definition of systems thinking: A systems approach. *Procedia Computer Science, 44,* 669–678. Retrieved from https://www.journals.elsevier.com/procedia-computer-science

Artur, S. (2018). How to increase the information assurance in the information age. *Journal of Defense Resources Management, 9*(1), 45–57. Retrieved from http://www.jodrm.eu/

Astani, M., Ready, K., & Tessema, M. (2013). BYOD issues and strategies in organizations. *Issues in Information Systems*, *14*(2), 195–201. Retrieved from https://www.iacis.org/iis/iis.php

Athukorala, K., Głowacka, D., Jacucci, G., Oulasvirta, A., & Vreeken, J. (2016). Is exploratory search different? A comparison of information search behavior for exploratory and lookup tasks. *Journal of the Association for Information Science and Technology*, *67*, 2635-2651. doi:10.1002/asi.23617

Attaran, M., & Woods, J. (2018). Cloud computing technology: Improving small business performance using the Internet. *Journal of Small Business & Entrepreneurship*, *30*, 495–519. doi:10.1080/08276331.2018.1466850

Aurigemma, S., & Mattson, T. (2017). Privilege or procedure: Evaluating the effect of employee status on intent to comply with socially interactive information security threats and controls. *Computers & Security*, *66*, 218–234. doi:10.1016/j.cose.2017.02.006

Australian Department of Industry, Innovation, & Science. (2018). *Innovation*. Retrieved from https://www.business.gov.au/change-and-growth/innovation

Awiagah, R., Kang, J., & Lim, J. I. (2016). Factors affecting e-commerce adoption among SMEs in Ghana. *Information Development*, *32*, 815–836. doi:10.1177/0266666915571427

Bada, M., & Nurse, J. R. (2019). Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). *Information & Computer Security*, *27*, 393–410doi:10.1108/ICS-07-2018-0080

Bailey, L. F. (2014). The origin and success of qualitative research. *International Journal of Market Research*, *56*, 167–184. doi:10.2501/IJMR-2014-013

Baillette, P., & Barlette, Y. (2018). BYOD-related innovations and organizational change for entrepreneurs and their employees in SMEs: The identification of a twofold security paradox. *Journal of Organizational Change Management*, *31*, 839–851. doi:10.1108/JOCM-03-2017-0044

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

Barnhill, G. D., & Barnhill, E. A. (2015). Data security in qualitative research. In M. de Chesnay (Eds.), *Nursing research using data analysis: Qualitative designs and methods in nursing* (pp.11–19). New York, NY: Springer.

Bazeley, P. (2016). Mixed or merged? integration as the real challenge for mixed methods. *Qualitative Research in Organizations and Management, 11*, 189-194. doi:10.1108/QROM-04-2016-1373

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

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

Berry, C. T., & Berry, R. L. (2018). An initial assessment of small business risk management approaches for cybersecurity threats. *International Journal of Business Continuity and Risk Management, 8*(1), 1–10. doi:10.1504/IJBCRM.2018.090580

Bertalanffy, L. (1968). *General systems theory: Foundations, development, application.* New York, NY: George Braziller.

Birt, L., Scott, S., Cavers, D., Campbell, C., & Walter, F. (2016). Member checking: A tool to enhance trustworthiness or merely a nod to validation? *Qualitative Health Research, 26*, 1802–1811. doi:10.1177/1049732316654870

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

Bogers, M., Zobel, A. K., Afuah, A., Almirall, E., Brunswicker, S., Dahlander, L., & Hagedoorn, J. (2017). The open innovation research landscape: Established perspectives and emerging themes across different levels of analysis. *Industry and Innovation, 24*(1), 8–40. doi:10.2139/ssrn. 2817865

Boiko, A., & Shendryk, V. (2017). System integration and security of information systems. *Procedia Computer Science, 104,* 35–42. doi.org/10.1016/j.procs.2017.01.053

Booth, A., Sutton, A., & Papaioannou, D. (2016). *Systematic approaches to a successful literature review*. London, England: Sage Publications.

Branch, L. E., Eller, W. S., Bias, T. K., McCawley, M. A., Myers, D. J., Gerber, B. J., … & Bassler, B. J. (2019). Trends in malware attacks against united states healthcare organizations, 2016-2017. *Global Biosecurity,* (1), 15. doi:org/10.31646/gbio.7

Bronnenmayer, M., Wirtz, B. W., & Göttel, V. (2016). Determinants of perceived success in management consulting: An empirical investigation from the consultant perspective. *Management Research Review, 39,* 706-738. doi:10.1007/s11846-014-0137-5

Brumen, B. (2019). Security analysis of game changer password system. *International Journal of Human - Computer Studies*, 126, 44–52. doi:10.1016/j.ijhcs.2019.01.004

Bungay, V., Oliffe, J., & Atchison, C. (2016). Addressing underrepresentation in sex work research: Reflections on designing a purposeful sampling strategy. *Qualitative Health Research, 26*, 966-978. doi:10.1177/1049732315613042

Burdon, M., & Coles-Kemp, L. (2019). The significance of securing as a critical component of information security: An Australian narrative. *Computers & Security, 87* (2019), 1-10. doi:10.1016/j.cose.2019.101601

Burns, E., Fenwick, J., Schmied, V., & Sheehan, A. (2012). Reflexivity in midwifery research. *Midwifery, 28*, 52–60. doi:10.1016/j.midw.2010.10.018

Butler, R., & Butler., M. (2018). Some password users are more equal than others: Towards customisation of online security initiatives. *South African Journal of Information Management*, *20*, 1-10. doi:10.4102/sajim.v20i1.920

Caldwell, T. (2016). Making security awareness training work. *Computer Fraud & Security, 16*(6), 8–14. doi:10.1016/S1361-3723(15)30046-4

Campbell, J., Ma, W., & Kleeman, D. (2011). The impact of restrictive composition policy on user password choices. *Behavior & Information Technology, 30*, 379–388. doi:10.1080/0144929X.2010.492876

Cappellaro, G. (2017). Ethnography in public management research: A systematic review and future directions. *International Public Management Journal, 20*, 14-48. doi:10.1080/10967494.2016.1143423

Carayon, P., Hancock, P., Leveson, N., Noy, I., Sznelwar, L., & van Hootegem, G. (2015). Advancing a sociotechnical systems approach to workplace safety: Developing the conceptual framework. *Ergonomics*, *58*, 548–564. doi:10.1080/00140139.2015.1015623

Carmichael, T., & Cunningham, N. (2017). Theoretical data collection and data analysis with gerunds in a constructivist grounded theory study. *Electronic Journal of Business Research Methods*, *15*(2), 59-73. Retrieved from www.ejbrm.com/

Castillo-Montoya, M. (2016). Preparing for interview research: The interview protocol refinement framework. *Qualitative Report*, *21*, 811-831. Retrieved from http://nsuworks.nova.edu/tqr/vol21/iss5/2

Catuogno, L., & Galdi, C. (2014). Analysis of a two-factor graphical password scheme. *International Journal of Information Security*, *13*, 421–437. doi:10.1007/s10207-014-0228-y

Ceric, A. (2015). Bringing together evaluation and management of ICT value: A systems theory approach. *Electronic Journal of Information Systems Evaluation*, *18*, 19–35. Retrieved from http://www.ejise.com

Chakraborty, R., Lee, J., Bagchi-Sen, S., Upadhyaya, S., & Raghav Rao, H. (2016). Online shopping intention in the context of data breach in online retail stores: An examination of older and younger adults. *Decision Support Systems*, *83*, 47–56. doi:10.1016/j.dss.2015.12.007

Chandani, Y., Duffy, M., Lamphere, B., Noel, M., Heaton, A., & Andersson, S. (2017). Quality improvement practices to institutionalize supply chain best practices for iCCM: Evidence from Rwanda and Malawi. *Research in Social and Administrative Pharmacy.Advance online publication 13*(6):1095-1109. doi:10.1016/j.sapharm.2016.07.003

Chandra, Y., & Shang, L. (2017). An RQDA-based constructivist methodology for qualitative research. *Qualitative Market Research, 20*, 90-112. doi:10.1108/QMR02-2016-0014

Chang, V. (2015). Towards a big data system disaster recovery in a private cloud. *Ad Hoc Networks, 35*, 65–82. doi:10.1016/j.adhoc.2015.07.012

Chaudhary, S., Schafeitel-Tähtinen, T., Helenius, M., & Berki, E. (2019). Usability, security, and trust in password managers: A quest for user-centric properties and features. *Computer Science Review, 33*(1), 69–90. doi:10.1016/j.cosrev.2019.03.002

Chen, Y., Lopez, L., Martinez, J.-F., & Castilleio, P. (2018). A lightweight privacy protection user authentication and key agreement scheme tailored for the internet of things environment: LightPriAuth. *Journal of Sensors, 2018*.1–16. doi:10.1155/2018/7574238

Cho, V., & Ip, W. H. (2018). A study of BYOD adoption from the lens of threat and coping appraisal of its security policy. *Enterprise Information Systems, 12*, 659–673. doi:10.1080/17517575.2017.1404132

Chuang, P. J., & Wang, C. H. (2017). An efficient group-based data backup and recovery scheme in cloud computing systems. *Journal of Information Science & Engineering, 33*(1). Retrieved from http://jise.iis.sinica.edu.tw/

Cibangu, S. K., & Hepworth, M. (2016). The uses of phenomenology and phenomenography: A critical review. *Library & Information Science Research, 38*, 148-160. doi:10.1016/j.lisr.2016.05.001

Clapper, D., & Richmond, W. (2016). Small business compliance with PCI DSS. *Journal of Management Information and Decision Sciences, 19*, 54–67. Retrieved from https://www.abacademies.org/journals/journal-of-management-information-and-decision-sciences-home.html

Colangelo, A. (2016). A systems theory of fragmentation and harmonization. *New York University Journal of International Law & Politics, 49*(1), 1–6. Retrieved from http://www.law.nyu.edu/

Coleman, S., Göb, R., Manco, G., Pievatolo, A., Tort-Martorell, X., & Reis, M. S. (2016). How can SMEs benefit from big data? Challenges and a path forward. *Quality and Reliability Engineering International*, *32*, 2151–2164. doi:10.1002/qre.2008.

Comert, M. (2018). A qualitative research on the contribution of in-service training to the vocational development of teachers. *Journal of Education and Training Studies, 6*, 114–129. Retrieved from http://redfame.com/journal/index.php/jets

Connelly, L. M. (2016). Understanding research. Trustworthiness in qualitative research. *MEDSURG Nursing*, *25*(6), 435-436. Retrieved from http://www.medsurgnursing.net/cgi-bin/WebObjects/MSNJournal.woa

Cornelissen, J. P. (2017). Preserving theoretical divergence in management research: Why the explanatory potential of qualitative research should be harnessed rather than suppressed. *Journal of Management Studies, 54*, 368-383. doi:10.1111/joms.12210

Counsell, A., Cribbie, R. A., & Harlow, L. L. (2016). Increasing literacy in quantitative methods: The key to the future of Canadian psychology. Canadian *Psychology/Psychologie Canadienne, 5*, 193-201. doi:10.1037/cap0000056

Cram, W. A., D, A. J., & Proudfoot, J. G. (2019). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly*, *43*(2), 525–554. doi:10.25300/MISQ/2019/15117

Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry & research design: Choosing among five approaches* (4th ed.). Los Angeles, CA: Sage.

Crossler, R. E., Long, J. H., Loraas, T. M., & Trinkle, B. S. (2017). The impact of moral intensity and ethical tone consistency on policy compliance. *Journal of Information Systems*, *31*, 49–64. doi:10.2308/isys-51623

Cuervo-Cazurra, A., Andersson, U., Brannen, M., Nielsen, B., & Rebecca Reuber, A. (2016). From the editors: Can I trust your findings? Ruling out alternative explanations in international business research. *Journal of International Business Studies, 47,* 881-897. doi:10.1057/s41267-016-0005-4

Culnan, M. J. (2019). Policy to avoid a privacy disaster. *Journal of the Association for Information Systems*, *20*, 848–856. doi:10.17705/1jais.00554

Curtis, S. R., Carre, J. R., & Jones, D. N. (2018). Consumer security behaviors and trust following a data breach. *Managerial Auditing Journal*, *33,* 425–435. doi:10.1108/MAJ-11-2017-1692

Dadkhah, M., Lagzian, M., & Borchardt, G. (2018). Academic information security researchers: Hackers or specialists? *Science and Engineering Ethics*, *24*(2), 785–790. doi:10.1007/s11948-017-9907-1

Damani, Z., MacKean, G., Bohm, E., Noseworthy, T., Wang, J. H., DeMone, B., ... Marshall, D. A. (2018). Insights from the design and implementation of a singleentry model of referral for total joint replacement surgery: Critical success factors and unanticipated consequences. *Health Policy*, *122*, 165-174. doi:10.1016/j.healthpol.2017.10.006

Das, G., Cheung, C., Nebeker, C., Bietz, M., & Bloss, C. (2018). Privacy policies for apps targeted toward youth: Descriptive analysis of readability. *JMIR mHEALTH and uHEALTH*, *6*(1), e3. doi:10.2196/mhealth.7626

Davidson, D., & Turmel, S. (2017). “Chipping” in for consumer protection or chipping away at small business? *Southern Law Journal*, *27*, 51–63. doi:10.1080/09638237.2018.1466051

Dawson, E., Hartwig, M., Brimbal, L., & Denisenkov, P. (2017). A room with a view: Setting influences information disclosure in investigative interviews. *Law & Human Behavior, 41*, 333–343. doi:10.1037/lhb0000244

Deane, J. K., Goldberg, D. M., Rakes, T. R., & Rees, L. P. (2019). The effect of information security certification announcements on the market value of the firm. *Information Technology and Management, (20)*, 107–121. doi:10.1007/s10799-018-00297-3 de las Cuevas, C., & Peñate, W. (2015). Psychometric properties of the eight-item morisky medication adherence scale (MMAS-8) in a psychiatric outpatient setting. *International Journal of Clinical and Health Psychology, 15,* 121–129. doi:10.1016/j.ijchp.2014.11.003

Demay, G., Gaži, P., Maurer, U., & Tackmann, B. (2019). Per-session security: Password-based cryptography revisited. *Journal of Computer Security*, *27*(1), 75–111. doi:10.3233/JCS-181131

Demetis, D. S. (2018). Fighting money laundering with technology: A case study of Bank X in the UK. *Decision Support Systems, 105*, 96–107. doi:10.1016/j.dss.2017.11.005

Dewasiri, N. J., Weerakoon, Y. K., & Azeez, A. A. (2018). Mixed methods in finance research: The rationale and research designs. *International Journal of Qualitative Methods*, *17*, 1-13. doi:1609406918801730

Dhingra, M. (2016). Legal issues in secure implementation of bring your own device (BYOD). *Procedia Computer Science*, *78*, 179–184. doi:10.1016/j.procs.2016.02.030

Dodgson, J. E. (2017). About research: Qualitative methodologies. *Journal of Human Lactation, 33*, 355–358. doi.org/10.1177/0890334417698693

Dominici, G. (2017). Governing business systems: Theories and challenges for systems thinking in practice. *Systems Research and Behavioral Science*, *34,* 310–312. doi:10.1002/sres.2454

Elhai, J., & Hall, B. (2016). Anxiety about Internet hacking: Results from community sample. *Computers in Human Behavior, 54*, 180–185. doi:10.1016/j.chb.2015.07.057

Esiner, E., & Datta, A. (2019). Two-factor authentication for trusted third party free dispersed storage. *Future Generation Computer Systems, 90*, 291–306. doi:10.1016/j.future.2018.08.001

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics, 5*(1), 1-4. doi:10.11648/j.ajtas.20160501.11

Fàbregues, S., & Molina-azorín, J. F. (2017). Addressing quality in mixed methods research: A review and recommendations for a future agenda. *Quality and Quantity, 51*, 2847-2863. doi:10.1007/s11135-016-0449-4

Federal Trade Commission. (2015). *Wyndham settles FTC charges it unfairly placed consumers' payment card information at risk.* [Press release]. Retrieved from https://www.ftc.gov/news-events/press-releases/2015/12/wyndham-settles-ftc-charges-it-unfairly-placed-consumers-payment

Federal Trade Commission. (2019). *Cybersecurity for small businesses: Cybersecurity basics.* Retrieved from https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/basics

Feng, N., Chen, Y., Feng, H., Li, D., & Li, M. (2019). To outsource or not: The impact of information leakage risk on information security strategy. *Information & Management.* doi:10.1016/j.im.2019.103215

Feng, N., Wang, M., Li, M., & Li, D. (2019). Effect of security investment strategy on the business value of managed security service providers. *Electronic Commerce Research and Applications, 35* [100843], 1-16. doi: 10.1016/j.elerap.2019.100843

Ferreira, F. A., & dos Santos, C. C. (2016). Possibilities of the phenomenological approach and of philosophical hermeneutics in type search state of art. *Philosophy of Mathematics Education Journal, 2016* (31), 1-4. Retrieved from www.philmath-europe.org

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

Frazer, L. (2016). Internal control: Is it a benefit or fad to small companies? A literature dependency perspective. *Journal of Accounting and Finance*, *16*, 149–161. Retrieved from http://www.na-businesspress.com/jafopen.html

Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report*, *20*, 1408–1416. doi:10.1080/08941920.2014.888791

Gao, C., Ma, J., Guo, J., Zhang, L., & Ma, X. (2013). The inside of information security industry in the perspective of hackers and economics. *Journal of Engineering Science and Technology Review*, *6*(3), 146–152. Retrieved from http://www.jestr.org/

Garcia, B., Welford, J., & Smith, B. (2016). Using a smartphone app in qualitative research: The good, the bad, and the ugly. *Qualitative Research, 16,* 508–525. doi: 10.1177/1468794115593335

Gauche, C., de Beer, L. T., & Brink, L. (2017). Managing employee well-being: A qualitative study exploring job and personal resources of at-risk employees. *South African Journal of Human Resource Management, 15*(1), 1-13. doi:10.4102/sajhrm.v15i0.957

Gerow, J., Thatcher, J., & Grover, V. (2015). Six types of IT-business strategic alignment: An investigation of the constructs and their measurement. *European Journal of Information Systems, 24,* 465–491. doi:10.1057/ejis.2014.6

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

Gi-Chul, Y. (2019). Development status and prospects of graphical password authentication system in korea. *KSII Transactions on Internet & Information Systems, 13*(11), 5755 - 5722. Retrieved from http://www.itiis.org/

Githinji, R. M., & Were, S. (2018). Challenges of implementing e-procurement in the ministry of transport, infrastructure, housing and urban development in Nairobi, Kenya. *Journal of Procurement & Supply Chain*, *2*(1), 1–13. Retrieved from https://stratfordjournals.org/

Gordon, L. A., Loeb, M., Lucyshyn, W., & Zhou, L. (2018). Empirical evidence on the determinants of cybersecurity investments in private sector firms. *Journal of Information Security*, *9*, 133–153. doi:10.4236/jis.2018.92010

Gordon, L. A., Loeb, M. P., & Zhou, L. (2016). Cybersecurity: Insights from the Gordon-Loeb model. *Journal of Information Security*, *7*, 49–59. doi:10.4236/jis.2016.72004

Gozman, D., & Willcocks, L. (2018). The emerging cloud dilemma: Balancing innovation with cross-border privacy and outsourcing regulations. *Journal of Business Research*, *97*, 235–256. doi: 10.1016/j.jbusres.2018.06.006

Graci, M. E., & Fivush, R. (2017). Narrative meaning making, attachment, and psychological growth and stress. *Journal of Social and Personal Relationships, 34,* 486-509. doi:10.1177/0265407516644066

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

Greenwood, M., Kendrick, T., Davies, H., & Gill, F. J. (2017). Hearing voices: Comparing two methods for analysis of focus group data. *Applied Nursing Research*, *35,* 90–93. doi: 10.1016/j.apnr.2017.02.024

Guo, Y., Zhang, Z., & Guo, Y. (2019). Optiwords: A new password policy for creating memorable and strong passwords. *Computers & Security*, *85*, 423–435. doi:10.1016/j.cose.2019.05.015

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

Haimes, Y. Y., Horowitz, B. M., Guo, Z., Andrijcic, E., & Bogdanor, J. (2015). Assessing systemic risk to cloud-computing technology as complex interconnected systems of systems. *Systems Engineering*, *18,* 284–299. doi:10.1002/sys.21303

Halabi, T., & Bellaiche, M. (2017). Towards quantification and evaluation of security of Cloud Service Providers. *Journal of Information Security and Applications, 33,* 55-65. doi:10.1016/j.jisa.2017.01.007

Hallova, M., Polakovic, P., Silerova, E., & Slocakova, I. (2019). Data protection and security in SMEs under enterprise infrastructure. *Agris On-Line Papers in Economics & Informatics*, 11(1). Retrieved from https://online.agris.cz/

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

Hammond, D. (2016). Special issue: General systems transdisciplinary. *Systema, 4*(1), 1–3. Retrieved from http://www.systema-journal.org/index

Harmouch, Y., & El Kouch, R. (2019). The benefit of using chaos in key schedule algorithm. *Journal of Information Security and Applications, 45,* 143–155. doi: 10.1016/j.jisa.2019.02.001

Harrison, J. S., Banks, G. C., Pollack, J. M., O'Boyle, E. H., & Short, J. (2017). Publication bias in strategic management research. *Journal of Management*, *43,* 400–425. doi.org/10.1177/0149206314535438

Heath, J., Williamson, H., Williams, L., & Harcourt, D. (2018). "It's just more personal": Using multiple methods of qualitative data collection to facilitate participation in research focusing on sensitive subjects. *Applied Nursing Research*, *43,* 30–35. doi:10.1016/j.apnr.2018.06.015

Hense, C., & McFerran, K. S. (2016). A critical grounded theory. (2016). *Qualitative Research Journal, 16*, 75-101. doi:10.1108/QRJ-08-2015-0073

Hess, M. F., & Cottrell, J. H., Jr. (2016). Fraud risk management: A small business perspective. *Business Horizons*, *59,* 13–18. doi:10.1016/j.bushor.2015.09.005

Hester, A. J. (2014). Socio-technical systems theory as a diagnostic tool for examining underutilization of wiki technology. *The Learning Organization, 21*, 48–68. doi:10.1108/TLO-10-2012-0065

Hina, S., Panneer Selvam, D. D. D., & Lowry, P. B. (2019). Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world. *Computers & Security, 87* (2019), 1-151. doi:/10.1016/j.cose.2019.101594

Hizam, S. M., & Amin, M. (2019). Towards economic growth: The impact of information technology on performance of SMES. *Journal of Security & Sustainability Issues, 9,* 241–255. doi:10.9770/jssi.2019.9.1(18)

Hoolachan, J. (2016). Ethnography and homelessness research. *International Journal of Housing Policy, 16*, 31-49. doi:10.1080/14616718.2015.1076625

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

Hughes, B. P., Newstead, S., Anund, A., Shu, C. C., & Falkmer, T. (2015). A review of models relevant to road safety. *Accident Analysis & Prevention, 74*, 250–270. doi:10.1016/j.aap.2014.06.003

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

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

Ip, F. C. F., Zhao, Y. M., Chan, K. W., Cheng, E. Y. L., Tong, E. P. S., Chandrashekar, O., ... & Ip, N. Y. Y. (2016). Neuroprotective effect of a novel Chinese herbal decoction on cultured neurons and cerebral ischemic rats. *BMC complementary and alternative medicine*, *16*(1), 437. doi.org/10.1186/s12906-016-1417-1

Jackson, D. R. (2018). Orchestrating the responses between information security and privacy during a data breach. *ISSA Journal*, *16*(3), 29–33. Retrieved from https://www.issa.org/page/ISSAJournal

Jamshed, S. (2014). Qualitative research method interviewing and observation. *Journal of Basic and Clinical Pharmacy, 5*, 87–88. doi:10.4103/0976-0105.141942

Jin, Y., Pang, A., & Smith, J. (2018). Crisis communication and ethics: The role of public relations. *Journal of Business Strategy, 39,* 43-52. doi:10.1108/JBS-09-2016-0095

Johnson, M., O’Hara, R., Hirst, E., Weyman, A., Turner, J., Mason, S., ... & Siriwardena, A. N. (2017). Multiple triangulation and collaborative research using qualitative methods to explore decision making in pre-hospital emergency care. *BMC Medical Research Methodology, 17*(1), 1-11. doi:10.1186/s12874-017-0290-z

Joslin, R., & Müller, R. (2016). The relationship between project governance and project success. *International Journal of Project Management*, *34,* 613-626. doi:10.1016/j.ijproman.2016.01.008

Juneja, K. (2020). An XML transformed method to improve effectiveness of graphical password authentication. *Journal of King Saud University - Computer & Information Sciences, 32*(1), 11. doi.org/10.1016/j.jksuci.2017.07.002

Kaleta, J., Lee, J., & Yoo, S. (2019). "Nudging with construal level theory to improve online password use and intended password choice". *Information Technology & People*, *32,* 993-1020. doi:10.1108/ITP-01-2018-0001

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

Kara, H., & Pickering, L. (2017). New directions in qualitative research ethics. *International Journal of Social Research Methodology, 20*, 239-241. doi:10.1080/13645579.2017.1287869

Karanja, E., & Rosso, M. A. (2017). The chief information security officer: An exploratory study. *Journal of International Technology and Information Management*, *26*(2), 23–47. doi:10.17705/1PAIS.10303

Katina, P. F. (2016). Metasystem pathologies (M-Path) method: Phases and procedures. *Journal of Management Development, 35*, 1287–1301. doi:10.1108/JMD-02-2016-0024

Kauspadiene, L., Ramanauskaite, S., & Cenys, A. (2019). Information security management framework suitability estimation for small and medium enterprise. *Technological & Economic Development of Economy, 25*(5), 979–997. doi:10.3846/tede.2019.10298

Keikha, A., Hoveida, R., & Nour, M. Y. (2017). The development of an intelligent leadership model for state universities. *Foresight and STI Governance, 11*(1), 66-74. doi:10.17323/2500-2597.2017.1.66.74

Khalili, M., Zhang, M., Borbor, D., Wang, L., Scarabeo, N., & Zamor, M.-A. (2018). Monitoring and improving managed security services inside a security operation center. *EAI Endorsed Transactions on Security & Safety, 5*(18), 1–20. doi:10.4108/eai.8-4-2019.157413

Kim, B.-H., Kim, K.-C., Hong, S.-E., & Oh, S.-Y. (2017). Development of cyber information security education and training system. *Multimedia Tools & Applications, 76*, 6051–6064. doi:10.1007/s11042-016-3495-y

Kim, J., Vetter, J. S., Dongarra, J., & Tourancheau, B. (2019). Implementing efficient data compression and encryption in a persistent key-value store for HPC.

International Journal of High Performance Computing Applications, 33, 1098–1112. doi:10.1177/1094342019847264

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

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

Kourti, I. (2016). Using personal narratives to explore multiple identities in organisational contexts. *Qualitative Research in Organizations and Management, 11*, 169-188. doi:10.1108/QROM-02-2015-1274

Kretser, M. P., Ogden, J. A., Colombi, J. M., & Hartman, P. L. (2016). Exploring design structure matrices to reduce enterprise information systems complexity. *Journal of Enterprise Transformation*, *6*, 39–59. doi:10.1080/19488289.2016.1217295

Lancaster, K. (2017). Confidentiality, anonymity and power relations in elite interviewing: Conducting qualitative policy research in a politicized domain. *International Journal of Social Research Methodology, 20*, 93-103. doi:10.1080/13645579.2015.1123555

Leclercq-Vandelannoitte, A. (2015). Managing BYOD: How do organizations incorporate user-driven IT innovations? *Information Technology & People*, *28*, 2–33. doi:10.1108/ITP-11-2012-0129

Leedy, P. D., Ormrod, J. E., & Johnson, L. R. (2019). *Practical research: Planning and design* (12th ed.). New York, NY: Pearson.

Lentz, J., Kennett, M., Perlmutter, J., & Forrest, A. (2016). Paving the way to a more effective informed consent process: Recommendations from the clinical trials transformation initiative. *Contemporary Clinical Trials, 49*, 65-69. doi:10.1016/j.cct.2016.06.005

Levitt, H. M., Pomerville, A., Surace, F. I., & Grabowski, L. M. (2017). Metamethod study of qualitative psychotherapy research on clients' experiences: Review and recommendations. *Journal of Counseling Psychology*, *64,* 626-644. doi:10.1037/cou0000222

Li, H., Luo, X., Zhang, J., & Sarathy, R. (2018). Self-control, organizational context, and rational choice in Internet abuses at work. *Information & Management*, *55*(3), 358–367. doi:10.1016/j.im.2017.09.00

Li, T., Vedula, S. S., Hadar, N., Parkin, C., Lau, J., & Dickersin, K. (2015). Innovations in data collection, management, and archiving for systematic reviews. *Annals of Internal Medicine, 162*, 287–294. doi:10.7326/M14-1603

Liao, C.-H., & Chen, M.-Y. (2019). Building social computing system in big data: From the perspective of social network analysis. *Computers in Human Behavior, 101*, 457–465. doi:10.1016/j.chb.2018.09.040

Liao, H., & Hitchcock, J. (2018). Reported credibility techniques in higher education evaluation studies that use qualitative methods: A research synthesis. *Evaluation & Program Planning*, *68,* 157-165. doi:10.1016/j.evalprogplan.2018.03.005

Liu, J. K., Liang, K., Susilo, W., Liu, J., & Xiang, Y. (2016). Two-factor data security protection mechanism for cloud storage system. *IEEE Transactions on Computers, 65*, 1992–2004. doi:10.1109/TC.2015.2462840

Loeb, S., Dynarski, S., McFarland, D., Morris, P., Reardon, S., & Reber, S. (2017). *Descriptive analysis in education: A guide for researchers* (NCEE 2017- 4023). Retrieved from http://ies.ed.gov/ncee/

Luborsky, M. R., & Lysack, C. (2017). *Design considerations in qualitative research*. In R. R. Taylor (Ed.), Kielhofner's research in occupational therapy: Methods of inquiry for enhancing practice (2nd ed., pp. 180-195). Philadelphia, PA: F. A. Davis.

Machi, L. A., & McEvoy, B. T. (2016). *The literature review: Six steps to success*. Thousand Oaks, CA: Corwin Press.

Madill, A., & Sullivan, P. (2017). Mirrors, portraits, and member checking: Managing difficult moments of knowledge exchange in the social sciences. *Qualitative Psychology, 5*, 1–20. doi:10.1037/qup0000089

Mansfield-Devine, S. (2012). Interview: BYOD and the enterprise network. *Computer Fraud & Security*, *2012*(4), 14–17. doi:10.1016/S1361-3723(12)70031-3

Marshall, C., & Rossman, G. (2016) *Designing Qualitative Research* (6th ed.). Thousand Oaks, CA: Sage Publications.

Mauceri, S. (2016). Integrating quality into quantity: Survey research in the era of mixed methods. *Quality and Quantity, 50*, 1213-1231. doi:10.1007/s11135-015-0199-8

Maughan, D., Balenson, D., Lindqvist, U., & Tudor, Z. (2015). Government-funded R&D to drive cybersecurity technologies. *IT Professional, 17*(4), 62–65. doi:10.1109/MITP.2015.70

Maxwell, J. A. (2016). Expanding the history and range of mixed methods research. *Journal of Mixed Methods Research, 10*, 12-27. doi.org/10.1177/1558689815571132

McPherson, H. (2014). Data privacy—Protecting this asset is a priority. *ISACA Journal*, *3*. Retrieved from https://www.isaca.org/

Merhi, M. I., & Ahluwalia, P. (2019). Examining the impact of deterrence factors and norms on resistance to Information Systems Security. *Computers in Human Behavior*, *92*, 37–46. doi:10.1016/j.chb.2018.10.031

Merriam, S. B., & Tisdell, E. J. (2016). *Qualitative research: A guide to design and implementation* (4th ed.). Hoboken, NJ: John Wiley & Sons.

Ming, X., Chen, Y., & Guo, J. (2019). Analysis of computer network information security and protection strategy. *MATEC Web of Conferences*. doi:10.1051/matecconf/201926702013

Miracle, V. A. (2016). The Belmont Report: The triple crown of research ethics. *Dimensions of Critical Care Nursing, 35*, 223–228. doi:10.1097/DCC.0000000000000186

Molina-Azorin, J. F., Bergh, D. D., Corley, K. G., & Ketchen, D. J. (2017). Mixed methods in the organizational sciences. *Organizational Research Methods, 20*, 179-192. doi:10.1177/1094428116687026

Moon, K., Brewer, T., Januchowski-Hartley, S., Adams, V., & Blackman, D. (2016). A guideline to improve qualitative social science publishing in ecology and conservation journals. *Ecology and Society, 21*(3), 17–36. doi:10.5751/ES-08663-210317

Morris, B., Rogaway, P., & Stegers, T. (2018). Deterministic encryption with the thorp shuffle. *Journal of Cryptology, 31*, 521–536. doi:10.1007/s00145-017-9262-z

Morrow, B. (2012). BYOD security challenges: Control and protect your most sensitive data. *Network Security*, *2012*(12), 5–8. doi:10.1016/S1353-4858(12)70111-3

Mubarak, S. (2016). Developing a theory-based information security management framework for human service organizations. *Journal of Information Communication and Ethics in Society, 14*, 254–271. doi:10.1108/JICES-06-2015-0018

Muthumeenakshi, R., Reshmi, T. R., & Murugan, K. (2017). Extended 3PAKE authentication scheme for value-added services in VANETs. *Computers and Electrical Engineering*, *59*, 27–38. doi:10.1016/j.compeleceng.2017.03.011

Mwangi, G., Chrystal, A., & Bettencourt, G. M. (2017). A qualitative toolkit for institutional research. *New Directions for Institutional Research, 2017*(174), 11-23. doi:10.1002/ir.20217

Nam, J., Kim, M., Choo, K.-K. R., & Paik, J. (2013). Dictionary attacks against password-based authenticated three-party key exchange protocols. *Transactions on Internet & Information Systems, 7*, 3244–3260. doi:10.3837/tiis.2013.12.016

Navab, A., Koegel, R., Dowdy, E., & Vernon, T. (2016). Ethical considerations in the application of the scientist-practitioner model for psychologists conducting intervention research. *Journal of Contemporary Psychotherapy*, *46*(1), 79-87. doi:10.1007/s10879-015-9314-3

Nguyen, T. H., Newby, M., & Macaulay, M. J. (2015). Information technology adoption in small business: Confirmation of a proposed framework. *Journal of Small Business Management, 53*, 207–227. doi:10.1111/jsbm.12058

Nico, L. M. (2016). Bringing life “back into life course research”: Using the life grid as a research instrument for qualitative data collection and analysis. *Quality & Quantity 50,* 2107–2120. doi.org/10.1007/s11135-015-0253-6

Nieles, M., Dempsey, K., & Pillitteri, V. (2017). *An introduction to information security*. Gaithersburg, MD: National Institute of Standards and Technology Special Publication

Nizamani, S. Z., Hassan, S. R., Shaikh, R. A., & Bakhsh, S. T. (2019). An evaluation model for recognition-based graphical password schemes. *Journal of Information Assurance & Security*, 14(3), 067–077. Retrieved from http://www.mirlabs.org/jias/

Noguerol, L. I., & Branch, R. (2018). Leadership and electronic data security within small businesses: An exploratory case study. *Journal of Economic Development Management IT, Finance, & Marketing*. Retrieved from https://gsmi-ijgb.com

Oleszkiewicz, S., Granhag, P. A., & Kleinman, S. M. (2017). Gathering human intelligence via repeated interviewing: Further empirical tests of the Scharff technique. *Psychology, Crime & Law, 23* (7), 1-28. doi:10.1080/1068316X.2017.1296150

Olivier, B. H. (2017). The use of mixed-methods research to diagnose the organisational performance of a local government. *SA Journal of Industrial Psychology, 43*(1), 1-14. doi.org/10.4102/sajip.v43i0.1453

Olufemi, A. (2019). Considerations for the adoption of cloud-based big data analytics in small business enterprises. *Electronic Journal of Information Systems Evaluation*, *21*, 63-79. Retrieved from http://www.ejise.com

Omune, O. G., & Kandiri, J. M. (2018). Hospital information systems capability and end-user satisfaction in hospitals of Nairobi County, Kenya. *International Academic Journal of Information Systems and Technology*, *2*(1), 102–125. Retrieved from https://www.iajournals.org/

Onwuegbuzie, A. J., & Byers, V. T. (2014). An exemplary for combining the collection, analysis, and interpretations of verbal and nonverbal data in qualitative research. *International Journal of Education*, *6*(1), 183–246. Retrieved from http://www.macrothink.org/journal/index.php/ije

Owoh, N. P., & Mahinderjit Singh, M. (2018). Security analysis of mobile crowd sensing applications. *Applied Computing and Informatics.* doi:10.1016/j.aci.2018.10.002

Panetto, H., Iung, B., Ivanov, D., Weichhart, G., & Wang, X. (2019). Challenges for the cyber-physical manufacturing enterprises of the future. *Annual Reviews in Control, 47*(2019), 1–25. doi:10.1016/j.arcontrol.2019.02.002

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, M., Kim, G., Park, Y., Lee, I., & Kim, J. (2019). Decrypting password-based encrypted backup data for Huawei smartphones. *Digital Investigation*, *28*, 119–125. doi:10.1016/j.diin.2019.01.008

Parker, L. D., & Northcott, D. (2016). Qualitative generalising in accounting research: Concepts and strategies. *Accounting, Auditing & Accountability Journal, 29,* 1100-1131. doi:10.1108/AAAJ-04-2015-2026

Parkhurst, J. (2017). Mitigating evidentiary bias in planning and policy-making. *International Journal of Health Policy and Management, 6*, 102-105. doi:10.15171/ijhpm.2016.96

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & Security*, *42*, 165–176. doi:10.1016/j.cose.2013.12.003

Patton, M. Q. (2015). *Qualitative research and evaluation methods* (4th ed.). Thousand Oaks, CA: Sage Publications.

Paulsen, C. (2016). Cybersecuring small businesses. *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

Peltier, T. R. (2016). *Information security policies, procedures, and standards: Guidelines for effective information security management*. Boca Raton, FL: CRC Press.

Pomare, C., & Berry, A. (2016). Integrative contingency-based framework of MCS: The 135 case of post-secondary education. *Journal of Accounting & Organizational Change, 12,* 351-385. doi:10.1108/JAOC-02-2014-0013

Porter, K., Wilfond, B., Danis, M., Taylor, H., & Cho, M. (2018). The emergence of clinical research ethics consultation: Insights from a national collaborative. *American Journal of Bioethics, 18*, 39-45. doi:10.1080/15265161.2017.1401156

Raghavan, K., Desai, M. S., & Rajkumar, P. V. (2017). Managing cybersecurity and ecommerce risks in small businesses. *Journal of Manangement Science and Business Intelligence*, 9-15. doi: 10.5281/zenodo.581691

Rahman, M. S. (2016). The advantages and disadvantages of using qualitative and quantitative approaches and methods in language “testing and assessment” research: A literature review. *Journal of Education and Learning, 6*(1), 102-112. doi:10.5539/jel.v6n1p102

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

Ramachandran, M., & Chang, V. (2016). Towards performance evaluation of cloud service providers for cloud data security. *International Journal of Information Management, 36*, 618–625. doi:10.1016/j.ijinfomgt.2016.03.005

Ramaswamy, M. (2019). Information technology strategies for small businesses. *Issues in Information Systems, 20*(2), 216. Retrieved from www.iacis.org

Rau, A. (2020). Dealing with feeling: Emotion, affect, and the qualitative research encounter. *Qualitative Sociology Review, 16*(1), 94–108. doi:10.18778/1733-8077.16.1.07

Renaud, K., Otondo, R., & Warkentin, M. (2019). "This is the way 'I' create my passwords"... does the endowment effect deter people from changing the way they create their passwords? *Computers & Security, 82*, 241–260. doi:10.1016/j.cose.2018.12.018

Reynolds, P., & Yetton, P. J. (2015). Aligning business and IT strategies in multi-business organizations. *Journal of Information Technology, 30,* 101–118. doi:10.1057/jit.2015.1

Ribeiro, E., Uhl, A., & Alonso-Fernandez, F. (2019). Iris super-resolution using CNNs: Is photorealism important to iris recognition? *IET Biometrics, 8*, 69–78. doi:10.1049/iet-bmt.2018.5146

Ridder, H. (2017). The theory contribution of case study research designs. *Business Research, 10*, 281-30

Robinson, M., Ford, S. L., & Goodman, L. B. (2018). An exploration of osteopaths' views and experiences regarding the identification of, and provision of advice for, urinary incontinence in women: A qualitative study using framework analysis. *International Journal of Osteopathic Medicine, 28*(2018), 20-29. doi:10.1016/j.ijosm.2018.03.004

Rohn, E., Sabari, G., & Leshem, G. (2016). Explaining small business InfoSec posture using social theories. *Information and Computer Security*, *24*, 534–556. doi:10.1108/ICS-09-2015-0041

Rojas-Mendez, J. I., Parasuraman, A., & Papadopoulos, N. (2017). Demographics, attitudes, and technology readiness: A cross-cultural analysis and model validation. *Marketing Intelligence & Planning, 35*(1), 18-39. doi: 10.1108/MIP-08-2015-0163

Rondi, E., De Massis, A., & Kotlar, J. (2018). Unlocking innovation potential: A typology of family business innovation postures and the critical role of the family system. *Journal of Family Business Strategy*. doi:10.1016/j.jfbs.2017.12.001

Rosenstein, R. (2017). *Deputy Attorney General Rod J. Rosenstein delivers remarks at the Global Cyber Security Summit.* Washington, DC: Department of Justice. Retrieved from https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-global-cyber-security-summit

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

Rossmiller, Z., Lawrence, C., Clouse, S., & Looney, C. (2017). Teaching an old dog new tricks: Disaster recovery in a small business context. *Information Systems Education Journal*, *15*(2), 13–19. Retrieved from https://jise.org/

Roulston, K. (2016). Issues involved in methodological analyses of research interviews. *Qualitative Research Journal, 16*, 68-79. doi:10.1108/QRJ-02-2015-0015

Rowley, J. (2016). Conducting research interviews. *Management Research Review, 35*, 260–271. doi:10.1108/01409171211210154

Roxas, F. M. Y., Rivera, J. P. R., & Gutierrez, E. L. M. (2019). Locating potential leverage points in a systems thinking causal loop diagram toward policy intervention. *World Futures, 75*, 609-631. Retrieved from https://www.tandfonline.com/toc/gwof20/current

Ruggunan, S. (2016). An exploratory study of the training of South African officers in the merchant navy. *Maritime Policy & Management*, *43*, 309-328. doi:10.1080/03088839.2015.1040861

Rumbold, J. M. M., & Pierscionek, B. K. (2017). A critique of the regulation of data science in healthcare research in the European union. *BMC Medical Ethic, 18*(1), 1-11. doi:10.1186/s12910-017-0184-y

Runfola, A., Perna, A., Baraldi, E., & Gregori, G. L. (2016). The use of qualitative case studies in top business and management journals: A quantitative analysis of recent patterns. *European Management Journal, 35*, 116-127. doi:10.1016/j.emj.2016.04.001

Sadiku, M. N. O., Alam, S., & Musa, S. M. (2017). Information assurance benefits and challenges: An introduction. *Information & Security, 36*(1). doi:10.11610/isij.3604

Safa, N., & Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior*, *57*, 442–451. doi:10.1016/j.chb.2015.12.037

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

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

San Nicolas-Rocca, T., & Burkhard, R. (2019). Information security in libraries: Examining the effects of knowledge transfer. *Information Technology & Libraries, 38*(2), 58–71. doi:10.6017/ital.v38i2.10973

Santos-Olmo, A., Sanchez, L. E., Caballero, I., Camacho, S., & Fernandez-Medina, E. (2016). The importance of the security culture in SMEs as regards the correct management of the security of their assets. *Future Internet*, *8*(3), 30. doi:10.3390/fi8030030

Sardone, N. B. (2017). Building bots to develop systems thinking. *Science Scope*, *40*(5), 32. Retrieved from https://www.nsta.org/middleschool/

Saulynas, S., Lechner, C., & Kuber, R. (2018). Towards the use of brain computer interface and gestural technologies as a potential alternative to PIN authentication. *International Journal of Human Computer Interaction*, *34*, 433–444. doi:10.1080/10447318.2017.1357905

Saunders, M. N., & Townsend, K. (2016). Reporting and justifying the number of interview participants in organization and workplace research. *British Journal of Management*, *27*, 836–852. doi:10.1111/1467-8551.12182

Sayin, H. U. (2016). A short introduction to system theory: Indispensable postulate systems and basic structures of the systems in quantum physics, biology, and neuroscience. *Neuroquantology, 14*, 126-142. doi:10.14704/nq.2016.14.1.855

Schatz, D., & Bashroush, R. (2019). Security predictions—A way to reduce uncertainty. *Journal of Information Security and Applications*, *45*, 107–116. doi.org/10.1016/j.jisa.2019.01.009

Schmitz, C., & Pape, S. (2020). LiSRA: Lightweight security risk assessment for decision support in information security. *Computers & Security*, *90* (2020), 1-27. doi:10.1016/j.cose.2019.101656

Schoenung, B., & Dikova, D. (2016). Reflections on organizational team diversity research: In search of a logical support to an assumption. *Equality, Diversity and Inclusion: An International Journal, 35*, 221-231, doi:10.1108/EDI-11-2015-0095

Sebescen, N., & Vitak, J. (2017). Securing the human: Employee security vulnerability risk in organizational settings. *Journal of the Association for Information Science & Technology*, *68*, 2237–2247. doi:10.1002/asi.23851

Seiler, J., & Kowalsky, M. (2011). Systems thinking evidence from colleges of business and their universities. *American Journal of Business Education, 4*, 55–62. doi:10.19030/ajbe.v4i3.4113

Shams, L., Sari, A. A., & Yazdani, S. (2016). Values in health policy -- a concept analysis. *International Journal of Health Policy & Management, 5*, 623-630. doi:10.15171/ijhpm.2016.102

Sharp, H., Dittrich, Y., & deSouza, C. R. (2016). The role of ethnographic studies in empirical software engineering. *IEEE Transactions on Software Engineering, 42*, 786-804. doi:10.1109/TSE.2016.2519887

Shi, T., & Guan, J. (2019). Cryptanalysis of the authentication in ACORN. *KSII Transactions on Internet & Information Systems, 13,* 4060–4075. doi:10.3837/tiis.2019.08.013

Singh, M. A. K. (2019). Digital library and its security issues: An overview. *Journal Current Science*, *20*(1). Retrieved from http://www.ijournal.scienceacad.com

Sivagnanam, M. (2018). Security measures that help reduce the cost of a data breach. *ISSA Journal*, *16*(10), 31–38. Retrieved from https://www.issa.org/page/ISSAJournal

Smith, K. T., Jones, A., Johnson, L., & Smith, L. M. (2019). Examination of cybercrime and its effects on corporate stock value. *Journal of Information, Communication and Ethics in Society*, *17*(1), 42-60. doi:10.1108/JICES-02-2018-0010

Soni, A., Pachouri, R., & Jain, A. (2018). PAKE protocol with OTSP and image based password authentication. *International Journal of Advanced Research in Computer Science, 9*, 858. doi:10.26483/ijarcs.v9i2.5894

Sperandei, S., Bastos, L. S., Ribeiro-Alves, M., & Bastos, F. I. (2018). Assessing respondent-driven sampling: A simulation study across different networks. *Social Networks, 52*, 48-55. doi:10.1016/j.socnet.2017.05.004

Subha, T., & Jayashri, S. (2017). Public auditing scheme for data storage security in cloud computing. *Journal of Information Science & Engineering, 33*, 773–787. doi:10.6688/JISE.2017.33.3.11

Sukamolson, S. (2016). *Fundamentals of quantitative research. EJTR*. Retrieved from https://independent.academia.edu/SSukamolson

Sundar, T. K. B., Løndal, K., Lagerløv, P., Glavin, K., & Helseth, S. (2018). Overweight adolescents' views on physical activity: Experiences of participants in an Internet-based intervention: A qualitative study. *BMC Public Health*, *18*, 448. doi:10.1186/s12889-018-5324-x

Sykes, B. L., Verma, A., & Hancock, B. H. (2018). Aligning sampling and case selection in quantitative-qualitative research designs: Establishing generalizability limits in mixed-method studies. *Ethnography*, *19*(2), 227–253. doi:10.1177/1466138117725341

Tadesse, A. F., & Murthy, U. S. (2018). Nonprofessional investor perceptions of the partial remediation of IT and non-IT control weaknesses: An experimental investigation. *International Journal of Accounting Information Systems*, *28,* 14–30. doi:10.1016/j.accinf.2017.12.001

Taguchi, N. (2018). Description and explanation of pragmatic development: Quantitative, qualitative, and mixed methods research. *Systems, 75*, 23-32. doi.org/10.1016/j.system.2018.03.010

Tisdale, S. M. (2015). Cybersecurity: Challenges from a systems, complexity, knowledge management, and business intelligence perspective. *Issues in Information Systems*, *16,* 191–198. Retrieved from https://www.iacis.org/iis/iis.php

Turner, S., & Endres, A. (2017). Strategies for enhancing small business owners' success rates. *International Journal of Applied Management and Technology, 16*(1), 3–18. doi:10.5590/IJAMT.2017.16.1.03

Twining, P., Heller, R. S., Nussbaum, M., & Tsai, C. (2016). Some guidance on conducting and reporting qualitative studies. *Computers & Education, 106* A1-9. doi:10.1016/j.compedu.2016.12.002

Uneke, C. J., Sombie, I., Lokossou, V., Johnson, E., & Ongolo-Zogo, P. (2017). An assessment of national maternal and child health policy-makers' knowledge and capacity for evidence- informed policy-making in Nigeria. *International Journal of Health Policy & Management, 6*, 309-316. doi:10.15171/ijhpm.2016.132

U.S. Department of Commerce. (2016a). *New NIST guide helps small businesses improve cybersecurity*. Gaithersburg, MD. Retrieved from https://www.nist.gov/news-events/news/2016/11/new-nist-guide-helps-small-businesses-improve-cybersecurity

U.S. Department of Commerce. (2016b). *Small business information security: The fundamentals*. Gaithersburg, MD. Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf

U.S. Department of Commerce. (2017a). *Small business cybersecurity: Federal resources and coordination*. Gaithersburg, MD. Retrieved from https://www.nist.gov/speech-testimony/small-business-cybersecurity-federal-resources-and-coordination

U.S. Department of Commerce. (2017b). *Information technology computer security resource center: Information assurance*. Retrieved from https://csrc.nist.gov/glossary/term/information-assurance

U.S. Department of Health & Human Services. (1979a). *Guidance on withdrawal of subjects from research: Data retention and other related issues.* Washington, DC. Retrieved from http://www.hhs.gov/ohrp/index.html

U.S. Department of Health & Human Services. (1979b). *The Belmont Report: Ethical principles and guidelines for the protection of human subjects of research.* Washington, DC. Retrieved from http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html

U.S. Department of Homeland Security. (2015a). *Contingency plan.* Washington, DC. Retrieved from https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=2ahUKEwippd3SmKPfAhVQEawKHaLHBFcQFjABegQIBBAC&url=https%3A%2F%2Fwww.dhs.gov%2Fsites%2Fdefault%2Ffiles%2Fpublic

ations%2FContingency%2520Plan%2520Extensible.docx&usg=AOvVaw3F2Kreg32zAwYdMVLft8s-

U.S. Department of Homeland Security. (2015b). *Stop. Think. Connect: National cybersecurity awareness campaign: Small business presentation*. Washington, DC. Retrieved from https://www.dhs.gov/sites/default/files/publications/Small%20Business%20Presentation.pdf

U.S. Department of Homeland Security. (2016). *IT disaster recovery plan.* Washington, DC. Retrieved from https://www.ready.gov/business/implementation/IT

U.S. Department of Homeland Security. (2018a). *Ready: IT disaster recovery plan.* Retrieved from https://www.ready.gov/business/implementation/IT

U.S. Department of Homeland Security. (2018b). *Stop. think. connect. small business resources*. Washington, DC. Retrieved from https://www.dhs.gov/publication/stopthinkconnect-small-business-resources#wcm-survey-target-id

U.S. Department of Homeland Security. (2019a). *Security Tip (ST04-001)*: *What is Cybersecurity?* Retrieved from https://www.us-cert.gov/ncas/tips/ST04-001

U.S. Department of Homeland Security. (2019b). *Security tip (ST04-020): Protecting portable devices: Data security*. Retrieved from https://www.us-cert.gov/ncas/tips/ST04-020

U.S. Department of Small Business Administration. (2018). *2018 small business profile: United States.* Washington, DC. Retrieved from https://www.sba.gov/sites/default/files/advocacy/2018-Small-Business-Profiles-US.pdf

U.S. Department of Small Business Administration. (2019). *Small business cybersecurity* Retrieved from https://www.sba.gov/business-guide/manage-your-business/small-business-cybersecurity#section-header-3

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management, 49,* 190–198. doi:10.1016/j.im.2012.04.002

Van den Berg, A., & Struwig, M. (2017). Guidelines for researchers using an adapted consensual qualitative research approach in management research. *Electronic Journal of Business Research Methods, 15*. 109–119. Retrieved from http://www.ejbrm.com/main.html

Vavilis, S., Petković, M., & Zannone, N. (2016). A severity-based quantification of data leakages in database systems. *Journal of Computer Security, 24*, 321–345. doi:10.3233/JCS-160543

Veleva, P. (2019). Personal data security for smart systems and devises with remote access. *Trakia Journal of Sciences, 17,* 873–882. doi:10.15547/tjs.2019.s.01.144

Vignesh, U., & Asha, S. (2015). Modifying security policies towards BYOD. *Procedia Computer Science, 50,* 511–516. doi: 10.1016/j.procs.2015.04.023

Volkova, V., & Kudriavtceva, A. (2018). Models for management of innovative activities on industrial enterprise. *Otkrytoe Obrazovanie, 22*, 64–73. doi:10.21686/1818-4243-2018-4-64-73

Wang, C., Xu, H., Li, G., & Chen, J. L. (2018). Community social responsibility and the performance of small tourism enterprises: Moderating effects of entrepreneurs' demographics. *International Journal of Tourism Research, 20,* 685. doi: 10.1002/jtr.2216

Wang, J., & Rusu, L. (2018). Factors hindering business-it alignment in small and medium enterprises in china. *Procedia Computer Science*, *138,* 425–432. doi:10.1016/j.procs.2018.10.060

Watts, L. L., Todd, E. M., Mulhearn, T. J., Medeiros, K. E., Mumford, M. D., & Connelly, S. (2017). Qualitative evaluation methods in ethics education: A systematic review and analysis of best practices. *Accountability in Research: Policies & Quality Assurance, 24,* 225-242. doi:10.1080/08989621.2016.1274975

West, J. L. (2017). A case of overcorrection: How the FTC's regulation of "unfair acts and practices" is unfair to small businesses. *William and Mary Law Review*, *58*, 2105. Retrieved from https://scholarship.law.wm.edu/wmblr/

Whitty, M., Doodson, J., Creese, S., & Hodges, D. (2015). Individual differences in cyber security behaviors: an examination of who is sharing passwords. *Cyberpsychology, Behavior, and Social Networking*, *18*(1), 3–7. doi.org/10.1089/cyber.2014.0179

Więcek-Janka, E., Mierzwiak, R., & Kijewska, J. (2016). The analysis of barriers in succession processes of family business with the use of grey incidence analysis (Polish perspective). *Naše Gospodarstvo/Our Economy*, *62*(2), 33–41. doi:10.1515/ngoe-2016-0010

Williams, J. C. (2015). A systems thinking approach to analysis of the Patient Protection and Affordable Care Act. *Journal of Public Health Management and Practice, 21*(1), 6–11. doi:10.1097/PHH.0000000000000150

Wilson, E., Kenny, A., & Dickson-Swift, V. (2018). Ethical challenges in communitybased participatory research: a scoping review. *Qualitative health research, 28*, 189-199. doi:10.1177/1049732317690721

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

Woods, N., & Siponen, M. (2018). Too many passwords? How understanding our memory can increase password memorability. *International Journal of Human-Computer Studies, 111*, 36–48. doi:10.1016/j.ijhcs.2017.11.002

Wu, Y., Fung, R. Y. K., Feng, G., & Wang, N. (2017). Decisions making in information security outsourcing: Impact of complementary and substitutable firms. *Computers & Industrial Engineering, 110*, 1–12. doi: 10.1016/j.cie.2017.05.018

Yadav, O. P., Nepal, B. P., Rahaman, M. M., & Lal, V. (2017). Lean implementation and organizational transformation: A literature review. *Engineering Management Journal, 29*(1), 2–16. doi:10.1080/10429247.2016.1263914

Yallop, A. C., & Mowatt, S. (2016). Investigating market research ethics. *International Journal of Market Research, 58,* 381-400. doi:10.2501/IJMR-2016-011

Yates, J., & Leggett, T. (2016). Qualitative research: An introduction. *Radiologic Technology*, 88, 225-231. Retrieved from http://www.radiologictechnology.org/content/88/2/225.extract

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

Yu, X., Wang, Z., Li, Y., Li, L., Zhu, W. T., & Song, L. (2017). EvoPass: Evolvable graphical password against shoulder-surfing attacks. *Computers & Security*, *70*, 179–198. doi:10.1016/j.cose.2017.05.006

Yuan, X., Williams, K., Rorrer, A., Chu, B. T., Yang, L., Winters, K., ... & Yu, H. (2017). Faculty workshops for teaching information assurance through hands-on exercises and case studies. *Journal of Information Systems Education*, *28*(1), 11. Retrieved from https://jise.org

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

Zahadat, N., Blessner, P., Blackburn, T., & Olson, B. A. (2015). BYOD security engineering: A framework and its analysis. *Computers & Security*, *55*, 81–99. doi:10.1016/j.cose.2015.06.011

Zauwiyah, A., Thian, S., Tze, H., & Mariati, N. (2019). Security monitoring and information security assurance behaviour among employees: An empirical analysis. *Information & Computer Security*, *27*, 165. doi:10.1108/ICS-10-2017-0073

Zhang, L. Z., Mouritsen, M., & Miller, J. R. (2019). Role of perceived value in acceptance of “Bring Your Own Device” policy. *Journal of Organizational and End User Computing (JOEUC), 31*(2), 65-82. Retrieved from https://www.igi-global.com/journal/journal-organizational-end-user-computing/1071

Zhao, P., Wu, L., Hong, Z., & Sun, H. (2019). Research on multicloud access control policy integration framework. *China Communications*, *16*(9), 222–234. doi:10.23919/JCC.2019.09.017

Zhu, Y. (2019). Combinatorial use of communication technologies in organizations. *Corporate Communications: An International Journal*, (4), 623. doi:10.1108/CCIJ-04-2018-0047

Zlatanovic, D., & Mulej, M. (2015). Soft-systems approaches to knowledge-cum-values management as innovation drivers. *Baltic Journal of Management*, *10*, 497–518. doi:10.1108/bjm-01-2015-0015

Appendix A: Interview Protocol

Date:

Location Options: Participant’s Company Location/Local Library

Interviewer:

Participant Pseudonym:

Set up electronic equipment prior to interviewing the participant.

Verify additional consent forms are onsite.

Begin introductions: My name is Sikini Knight. Thank you for coming. I will be facilitating this interview. Today’s date is (state the date). We are located at (state location).

Purpose of the interview: The purpose of this interview is to explore the strategies small business owners use to reduce data security breaches. There are no right or wrong answers.

Identify my connection to the study: For your awareness, I would like to disclose my connection to the study. My former professional career as a software engineer gives me a personal connection to the study. I have worked as an IT professional for more than 15 years. During my career, I have experienced personal security breaches.

Remind the participant that their identity is anonymous. I will assign you a code to conceal your identity. You can find the code at the top of your consent form. I will refer to you by your code for the remainder of the interview.

Get permission to record the interview: If it is okay with you, I will be recording our interview. The purpose of recording the interview is to ensure I capture your response accurately.

Explain member checking to the participant: I will contact you within one week to provide you with a transcribed copy of my notes to ensure I have captured your responses accurately. At that time, you will have one day to review the transcribed data collected during the interview. I will follow-up by phone to review the information with you and to answer any questions.

Assure the participant that their information will be confidential: I assure you that all your comments will remain confidential. I will be compiling data, which will contain all participants' comments without any reference to individuals.

Review consent form and have the participant acknowledge their consent

Collect a signed copy of the consent form:

Prior to the interview, you were sent a consent form please keep one for your copy, and I will keep the signed copy.

Check folder for signed consent form. Acknowledge if I do not have the signed consent form. If I do not have the consent form ask the participant, did you bring your consent letter? If not, I have one here for you. (Copies distributed). Do you have any questions?

Explain the duration of the interview: The interview will take approximately 45 to 60 minutes and will follow an interview protocol. There will be no incentives for participating in this interview.

If you are ready, let us begin with some background questions.

How long have you worked for the organization?

Do you use technology to conduct business within your organization?

Let us begin with the first research question.

1. What strategies did you use to reduce security breaches in your organization?
2. How is data security performance measured in your organization?
3. How would your organization address internal or external data security breaches?
4. How are you training your employees to protect your organization’s data from a data security breach?
5. How have your existing policies and procedures protected your organization’s data security environment against intrusions from outsiders and insiders (intentional or unintentional)?
6. How does your organization back up sensitive data?
7. What else can you add to help other business leaders reduce data security breaches?

Conclude interview. This concludes the interview. Thank you for participating. You will receive a transcribed copy of my notes within 1 week from today.

Appendix B: Recruitment Letter

Dear [*insert name*],

My name is Sikini Knight, and I am a student from the Department of Business at Walden University. I am writing to invite you to participate in my research study about the strategies needed by small business owners to reduce data security breaches. You're eligible to be in this study because you (a) own a small business in the southern region of the United States for at least 5 years , (b) less than 1500 employees, (c) use technology to conduct business, (d) have implemented data security strategies successfully, and (e) participate in the data security decision-making process to support your business. I obtained your contact information from [*describe source*].

If you decide to participate in this study, I will contact you by email or phone to set up an interview. Interviews are conducted by Skype or face-to-face in a private room at your organizational location or at the local library. I would like to audio record your interview and then we will use the information to take notes for the study. I will provide with a copy of my notes to verify that I have captured your responses appropriately. All participants will be anonymous.

Remember, this is voluntary. You can choose to be in the study or not. If you would like to participate or have any questions about the study, please email or contact me at sikini.knight@waldenu.edu or 228-334-2847

Thank you very much.

Sincerely,

Sikini Knight

Appendix C: Withdrawal Form

You have indicated that you would like to withdraw from the study. You have the right to withdraw fully from this study at any time, and you do not have to provide a reason. Information collected before signing this documentation may be used in the study. The information collected before a withdrawal will be coded with a series of letters and numbers to hide your identity. By signing this form, you agree that you have reviewed this form and understood the conditions.

I withdraw my consent for participation, in this study in accordance with the withdrawal option in the above statements.

Researcher Signature ____________________________________

Date __________________________

Signature of person obtaining consent _______________________________

Date ______________________

Printed name of person obtaining consent _______________________________

Date ______________________