Walden University
ScholarWorks

Walden Dissertations and Doctoral Studies

Walden Dissertations and Doctoral Studies Collection

2020

Strategies for Implementing Successful IT Security Systems in Small Businesses

Martins Donbruce Idahosa
Walden University

Follow this and additional works at: https://scholarworks.waldenu.edu/dissertations

 Part of the Databases and Information Systems Commons

This Dissertation is brought to you for free and open access by the Walden Dissertations and Doctoral Studies Collection at ScholarWorks. It has been accepted for inclusion in Walden Dissertations and Doctoral Studies by an authorized administrator of ScholarWorks. For more information, please contact ScholarWorks@waldenu.edu.

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Martins Donbruce Idahosa

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. Robert Banasik, Committee Chairperson, Doctor of Business Administration Faculty

Dr. Lisa Pearo, Committee Member, Doctor of Business Administration Faculty

Dr. Lisa Cave, University Reviewer, Doctor of Business Administration Faculty

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

Walden University
2020

Abstract

Strategies for Implementing Successful IT Security Systems in Small Businesses

by

Martins Donbruce Idahosa

MSIT, Kaplan University, 2015

MBA, Kaplan University, 2013

B. Sc IT, Purdue University Global, 2018

B.A.Sc., Broward College, 2011

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

April 2020

Abstract

Owners of small businesses who do not adequately protect business data are at high risk for a cyber attack. As data breaches against small businesses have increased, it has become a growing source of concern for consumers who rely on owners of small businesses to protect their data from data breaches. Grounded in general systems theory and routine activity approach, the focus of this qualitative multiple case study was to explore strategies used by owners of small businesses to protect confidential company data from cyber attacks. The process used for collecting data involved semistructured face-to-face interviews with 5 owners of small businesses in Florida, as well as a review of company documents that were relevant to strategies used by owners of small businesses to protect confidential company data from cyber attacks. The thematic analysis of the interview transcripts revealed 4 themes for protecting business data against cyber attacks, which are security information management strategy, organizational strategy, consistent security policy, and cybersecurity risk management strategy. A key finding is that owners of small businesses could develop an organizational strategy by incorporating procedures used to protect from and respond to cyber attacks. The implications for positive social change include the potential to increase customers' confidence and businesses' economic growth, as well as stimulate the socioeconomic lifecycle, resulting in potential employment gains for residents within the communities.

Strategies for Implementing Successful IT Security Systems in Small Businesses

by

Martins Donbruce Idahosa

MSIT, Kaplan University, 2015

MBA, Kaplan University, 2013

B. Sc IT, Purdue University Global, 2018

B.A.Sc., Broward College, 2011

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

April 2020

Dedication

I dedicate this research to my family: Ugochi, my wife, and my two children, Marvis and Ethan. Ugochi, you have been incredibly supportive as you have sacrificed our time together and allowed me to focus on this study. Without your constant affirmation and support, I would not have been able to complete this study. Marvis and Ethan, you have been more than understanding as I have spent countless hours in my study room researching and writing. My entire family has been so encouraging and supportive during this endeavor; I could not have done this without you. To my family, I am forever grateful.

Acknowledgments

I'd like to thank my lord and savior Jesus Christ for giving me the strength and zeal through this journey. I'd like to acknowledge my academic mentor, Dr. Robert Banasik, for his persistent guidance, support, and steadfast commitment to helping me succeed. He was always willing to make himself available to discuss the various elements involved in the process of bringing this study to life. He was always open and honest with his feedback, even when I did not want to hear it. I am thankful for Dr. Banasik's mentorship throughout this entire process. I also wish to thank my second committee members, Dr. Douglas Keevers, Dr. Lisa Pearo, and my URR, Dr. Lisa Cave for their constant support and feedback throughout this process. Lastly, my fellow cohorts who have also supported my study with their contributions.

Table of Contents

List of Tables

Section 1: Foundation of the Study

Cyber security threats have increased since the rise of technological advancements. Cyber attacks are a continuing threat, and when there is a breach of sensitive data, both organizations and consumers are affected (Balan, Otto, Minasian, & Aryal, 2017). Owners of small businesses have become more attractive targets because they lack the financial resources and Internet technology (IT) personnel to commit to cybersecurity like big companies (Selznick & Lamacchia, 2018). As data breaches against small businesses have increased, it has become a growing source of concern for consumers who rely on owners of small businesses to protect their data from data breaches. Therefore, I sought to understand what strategies owners of small businesses used to protect their business and customer information from cyber attacks.

Background of the Problem

Watad, Washah, and Perez (2018) noted that 79% of owners of small businesses have no plans to respond to a cyber attack, while 40% do not believe their businesses would be attacked. Owners of small businesses have been struggling to combat threats and protect company and customer data (Goode, Hoehle, Venkatesh, & Brown, 2017). Selznick and Lamacchia (2018) pointed out that 43% of cyber attacks in mid-2016 were targeted at small businesses. Cybersecurity issues are becoming more prevalent, with an increasing number of threats and vulnerabilities. Owners of small businesses lack effective cybersecurity strategies to protect their business and customer information from cyber attacks.

Problem Statement

The threat of cyber attacks to businesses in the United States is increasing as more businesses become targets for trade secrets, sensitive corporate data, and customer information (FBI, 2016a). The cost of data breaches to U.S. companies increased from $800,000 in 2014 (FBI, 2014) to $1.3 billion in 2016 (FBI, 2016b). The general business problem was that data breaches could damage a business brand reputation and cause customers to lose confidence. The specific business problem was that some owners of small businesses lack cyber defense strategies to protect business data from cyber attacks.

Purpose Statement

The purpose of this qualitative multiple case study was to explore strategies owners of small businesses used to protect confidential company data from cyber attacks. The target population for this study consisted of five successful owners of small businesses in the Fort Lauderdale, Florida area who have implemented effective cybersecurity strategies to protect their business data from cyber attacks. The implications for positive social change include the potential to enhance sound cybersecurity policy to reduce data breaches, and protect business and customer data, thereby increasing customers' confidence, increasing businesses' economic growth, and stimulating the socioeconomic lifecycle, resulting in potential employment gains for residents in communities.

Nature of the Study

I used a qualitative research methodology for this study. Researchers use qualitative methods to understand the underlying phenomena and motivation in real-life

situations and gain insight into research problems (Reinecke, Arnold, & Palazzo, 2016).

A qualitative methodology was appropriate to gain insights into the strategies some owners of small businesses use to protect confidential company data from cyber attacks. I reviewed other methodologies, such as quantitative and mixed methodologies. A quantitative research methodology was not suitable for this study because I did not intend to examine the relationships among variables. Researchers use the quantitative methodology for predicting, describing, and categorizing groups to consistently identify patterns (Elman, Gerring, & Mahoney, 2016). I rejected the mixed methods methodology because this study does not include relationships among variables. The mixed methodology involves collecting, analyzing, and integrating both qualitative and quantitative methodologies to solve a research problem (Reinecke et al., 2016).

A qualitative multiple case study was an appropriate design choice for this study because it was the process used to obtain data through semi structured interviews and company documentation. Researchers used multiple case studies to analyze data across different situations and build explanations from the collected information (Ridder, 2017). I reviewed other qualitative designs, such as ethnographic, phenomenological, and narrative designs. An ethnographic research design was unsuitable for this study because the goal of this study was not to understand the cultural practices of a specific group (Cardoso, Gontijo, & Ono, 2017). A phenomenological research design was inappropriate for this study because the goal was not to observe the meaning of experiences lived by a group or an individual that relates to a particular phenomenon (see Flynn & Korcuska, 2018). Using narrative research was not appropriate for this study because the

participants' descriptions of stories from their personal experiences may not be relevant. A narrative researcher provides a visual representation or written stories of the participants' personal experiences (Bruce, Beuthin, Sheilds, Molzahn, & Schick-Makaroff, 2016).

Research Question

The research question for this study was: "What strategies do owners of small businesses use to protect business data against cyber attacks?"

Interview Questions

The interview questions used to gather data for this study included the following:

1. Please describe the strategies and various security tools that your organizations currently utilize to address or mitigate targeted cyber attacks successfully?
2. How, if at all, do you conduct a security system assessment to ensure basic security practices are in place?
3. What successful processes have you implemented to implement your security awareness program?
4. What, if any, successful employee training have you implemented for security procedures to improve and enhance cyber attack detection capabilities?
5. How successful is your response plan for detecting, preventing and protecting both business and consumers' data?
6. What is your contingency plan in the event of a successful cyber–attack?
7. What successful data control techniques have you implemented?

8. What else can you tell me regarding how your business is protecting customers' data against cyber–attacks?

Conceptual Framework

I chose Von Bertalanffy's (1972) general systems theory (GST) and Cohen and Felson's (1979) routine activity approach (RAA) as the conceptual framework of this study. Von Bertalanffy (1972) developed the GST as an interdisciplinary theory to analyze the nature of complex systems, and as a framework, it is a process used to investigate any group of connected objects. The framework could serve as the basis for understanding complex cybersecurity systems and implement strategies to change their focus from defensive to offensive approaches (Stitilis, Pakutinskas, Kinis, & Malinauskaite, 2016).

Cohen and Felson (1979) developed the RAA and noted that crime happens when the following three elements are simultaneously present in any specified space and time: (a) a motivated offender, (b) a suitable target, and (c) the absence of a guardian. Leukfeldt and Yar (2016) noted that the RAA would be useful as an analytical framework to study cybercrimes, identify vulnerable targets, and serve as a means for adopting and enforcing cybersecurity policies.

Von Bertalanffy's (1972) GST and Cohen and Felson's (1979) RAA were both synthesized frameworks used to formulate a comprehensive cybersecurity strategy. Both theories aligned with this study. I integrated both theories into the conceptual framework through which I reviewed strategies used by owners of small businesses to protect business and customer data from cyber attacks.

Operational Definitions

The following terms were used throughout the study.

Cybercrime: A growing act that is directed at specific victim computers to generate profit for the cybercriminals (Huang, Siegel, & Madnick, 2018).

Cyber defense mechanisms: This is a collection of tools and concepts used for detecting and preventing attacks (Jones & Shashidhar, 2017).

Cybersecurity awareness: This is the combination of knowledge and techniques used to protect and prevent cyber attacks (Onwubiko, 2017).

Data leakage: This is the transfer of sensitive or classified data from a secured system to an unauthorized third party (Vavilis, Petkovic, & Zannone, 2016).

Information security threats: The various techniques hackers are using to compromise the integrity of an information system (Young, 2016).

Insider threat: An insider threat occurs when an employee gains control to abuse one or more rules outlined in the specified cybersecurity policy (Vlad-Mihai, 2017).

Online security breach: A deliberate and malicious act used to disrupt or breach an information system to gain access to individual or organization data (Trappe & Straub, 2018).

Security controls: These refer to any precautions or countermeasures that organizations use to avoid or minimize cybersecurity risks (Trappe & Straub, 2018).

Small business: Small businesses include private corporations, partnerships, or sole proprietorships with the size standard that ranges from 1 to 1,500 employees (SBA, 2018a).

Assumptions, Limitations, and Delimitations

Assumptions

Assumptions describe those elements that are out of the scope of the researcher but are considered and accepted as relevant to the study (Feller, Mealli, & Miratrix, 2017). There were two assumptions related to this study. The first assumption was that participants would answer the interview questions without fear of reprisal or harm to their reputation and business. I presented participants with confidentiality agreements to ease any fears of reprisal. The second assumption was that participants would honestly and truthfully answer questions regarding their business cybersecurity.

Limitations

Limitations describe those elements that are outside the researcher's control and can potentially create weaknesses in a study (Roseveare, 2017). The first limitation of this study was that owners of small businesses might unintentionally provide insufficient data due to their limited knowledge of cyber security. The second limitation was the continued growth of cyber security, which would limit the knowledge of participants.

Delimitations

Delimitations are the boundaries and limitations that the researcher sets to reduce the scope of the study's investigation (Park & Park, 2016). The delimitations of the study were the size of the business, the sample size, and the location of the businesses. I limited the study findings to specific small businesses located in the Fort Lauderdale, Florida area.

Significance of the Study

One of the most significant issues facing owners of small businesses is the ability to protect themselves against potential cyber attacks. When sensitive data is at risk, due to cyber attacks, both organizations and their customers are affected (Goode et al., 2017). A business' reputation suffers when business owners fail to protect data, which could lead to the loss of the business' customers (Janakiraman, Lim, & Rishika, 2018). Some owners of small businesses do not allocate budget items to mitigate and address cyber vulnerabilities. Owners of small businesses have an urgent need to develop effective cyber strategies to protect their company assets, intellectual property, and customer data from cyber attacks. The results of this study may help owners of small businesses develop cyber strategies to identify vulnerable targets and mitigate threats to protect companies' confidential data.

The findings of this study may include information that might be useful in formulating cyber security strategies that could help to predict and eliminate future threats to customers' information privacy problems. The implications for positive social change include the potential to develop and stimulate economic growth and create additional jobs to improve the social lifestyle of residents within communities.

A Review of the Professional and Academic Literature

I began my search of the literature by reviewing the conceptual framework of the GST and RAA. I discussed both frameworks and developed a comprehensive analysis and synthesis of sources from peer-reviewed journals, published dissertations, and government data. My search efforts focused on accessing information through Walden

University library resources, including the following databases: Emerald Management, Business Source Complete, ProQuest, Academic Search Complete, EBSCOhost, ABI/INFORM Complete, ACM Digital Library, IEEE Source Library, and SAGE Premier, a multi-discipline research database. I used the Ulrich web global serials directory database engine and the journal articles' homepages to validate the scholarly reference and peer-reviewed listings.

The literature review search criteria included the following keywords: *cyber attacks, cybersecurity threat, data breaches, strategies for data breaches, ransomware attack, cyber-crimes, internal and external breaches, cyber incidents, cyber fraud, network security monitoring, cyber hacking, cyber loss, data theft, cyber warfare, data loss, email phishing, hacking, fraud, network prevention, security prevention, risk assessments, government regulations for cyber security, security detection, software theft,* and *intrusion prevention and detection.*

At least 85% of the citations were from peer-reviewed and academic journals that were published within 5 years of the anticipated CAO approval date. Table 1 includes the various citations used in the study.

Table 1

The Breakdown for Literature Review Publication

	Total sources	Year published (2016-2020)	Percentage published 2016-2020	Peer-reviewed sources	Percentage peer-reviewed
Full document	233	208	85.30%	192	92.05%
Literature review	136	145	95.34%	134	98.53%

The purpose of this qualitative multiple case study was to explore strategies used by business owners to protect their business data from cyber attacks. Business and consumer data breaches have become a significant business problem. The objective of implementing cyber security strategies was to prevent unauthorized access and use of business and consumer data (Janakiraman et al., 2018). Stitilis et al. (2016) stated that cybersecurity breaches, intense cyber wars, and separate attacks are becoming more common than the physical attacks; such cybersecurity violations might result in damage to businesses' reputations. Densham (2015) noted that organizations must respond with a comprehensive plan to mitigate breaches and implement effective cybersecurity strategies to prevent a potential disaster.

I discuss the following concepts and key sectors further in the next sections: (a) evolution of theories, (b) theories supporting cybersecurity, (c) cybersecurity threats, (d) holistic cybersecurity strategies, (e) system security strategy, (f) intrusion detection strategy (g) cybersecurity awareness education and training, (h) outsourcing strategy, (i)

third-party vendors strategy, (j) holistic prevention strategy, (k) data protection strategy, (l) data breach prevention strategy, and (m) data leak prevention strategy.

Evolution of General System Theory

Von Bertalanffy (1972) developed an outline of GST by considering (a) system units, (b) collaborative exchange and continual relationships within the system, and (c) the analysis of systems would provide a way of interpreting and viewing interconnected units. Von Bertalanffy (1950) began by envisioning a theory and conceptual framework that would be equally applicable to many fields of inquiry. Wang, Shi, Nevo, Li, and Chen (2015) viewed an organization as a system that consists of subsystems working together in an ever-changing environment to achieve a common goal; any form of change or impact in one subsystem affects the overall system or organization. Von Bertalanffy (1969) argued that the GST bridges the gap by dividing subject and object-oriented disciplines. Rousseau (2015) added that the GST could be applied to support interdisciplinary collaboration and enable scientific findings in disciplines that lack such theories. The principle of systems theory is a process used to manage people and processes within an organizational environment (Rousseau, 2015). Bohm and Kuhn (1964) expanded the systems theory by suggesting that scientific progress is not a straightforward evolution, but a systematic application of methods where knowledge surges to the limits of the current model. Bohm and Kuhn concluded that one viewpoint replaces another, resulting in a shift and leading to the development of subsystems with dynamic and new characteristics.

Bennis, Katz, and Kahn (1966) developed an open-systems approach to repeated cycles of input, output, and throughput. Systems receive input as a form of resources from the environment; this input is processed into a system as throughput and produces output to restore the balance (Bennis et al., 1966). The open systems use this process as a means of interacting with the environment; this is a process used to define which components of the system are not operational as designed, thereby affecting the system (Anders, Schiendorfer, Siefert, Steghofer, & Reif, 2015). The fundamental premise of GST is that different system units tend to share some basic organizing principles, irrespective of their purposes, which contribute to system wholeness (Von Bertalanffy, 1972). Researchers can use GST to understand the wholeness of organization systems and to discuss leadership, management, and related functions.

Von Bertalanffy (1969) noted the holistic approach of the GST by implying that systems consist of interrelating parts; it is impossible to isolate the connections from the rest of the system by reviewing a single component. The only exceptions to this are (a) when the system interactions are weak and (b) when there is a linear relationship between the system components. The holistic approach changes the method by using the analytical tools to review network and security systems. The holistic system approach is a process used to set boundaries to problems while understanding the relationships within natural systems to avoid unwanted consequences (Monat & Gannon, 2018). Gajic, Palcic, and Cosic (2015) evaluated the influence of this approach, as a process used to examine systems as a complete functioning unit by depending on the following building blocks: (a) the foundations of GST, (b) cybernetics, and (c) soft system method. With these

building blocks, it is possible to define, investigate, and explain security (Gajic et al., 2015). In this study, I explored why a holistic system approach to cybersecurity is essential, especially regarding the prevention or mitigation of data breaches.

Von Bertalanffy (1972) indicated that systems could self-correct and regulate; as such, through this lens, we can understand complex problems and phenomena. GST through the lens of interdisciplinary, cross-cutting meta-concept that can evaluate current security and safety analysis techniques (Lei, Yang, Niu, Yang, & Hao, 2017). It is also possible through the lens of GST to identify issues within the system and solve problems related to identifying, restructuring, and optimizing security monitoring systems while considering multiple objectives, constraints, resources, benefits, costs, and risks (Tisdale, 2015).

Evolution of Routine Activity Approach (RAA)

Cohen and Felson (1979) developed the RAA, which explains that crime occurs during the instantaneous meeting of a motivated offender with an appropriate target that lacks capable guardians. Cohen and Felson (1979) indicated that one must evaluate all three components in a broader context before investigating them at a micro-level. The importance of the findings at the macro level provided the motivation needed for scholars and researchers to test the theory (Cohen & Felson, 1979). Many scholars and researchers have investigated the micro and macro levels while trying to explain offender behavior and criminal victimization (Savard, 2018).

Williams (2016) supported the argument that Internet governance is achievable with a combination of macro and micro guardianship as the controlling effect of

cybersecurity strategies. Scholars have used the RAA to focus on criminals' actions, rather than the criminals themselves, which makes this approach salient to studies of cybercrime (Williams, 2016). Argun and Daglar (2016) suggested that the RAA can be a useful theory for preventing and reducing crime. Practitioners can use this approach to evaluate and analyze criminal problems, as well as to recommend routine measures and precautions to reduce criminal opportunities. This perspective can aid the understanding of cyber attacks by focusing on specific cybercrime attacks and how such attacks affect guardianship and suitable targets (Leukfeldt & Yar, 2016).

Williams, Levi, Burnap, and Gundur (2018) noted that the RAA could provide potentially useful criminological insight into insider cyber victimization. The authors further indicated that insider cybersecurity breaches are a function of routine activities. Organizations, therefore, must be evaluated whether potential offenders are motivated and determine by a suitable target in the absence of guardianship (Williams et al., 2018).

Theories Supporting Cybersecurity

Monat and Gannon (2018) noted that systems share common characteristics, including a dynamic structure that can be defined by components and configuration. Integrated systems consist of several interacting elements involving processing inputs and producing outputs, interconnections between different functioning parts of the system, and structured relationships (Monat & Gannon, 2018). In a modern system, each level of information is related to a level of correspondent security risk. Each level must be well-defined, including a proper measure to control the risks of data security (Anton & Nedelcu, 2015). A systemic method is a process used to manage data security; the

process is based on understanding how a system's processes can effectively be structured to secure all components of the system (Anton & Nedelcu, 2015). A system mainly consists of integrated objects, either logical or physical, qualities that describe the objects, the objects' relationship with other objects, and the system's control environment (Gutierrez-Martinez, Nunez-Gaona, & Aguirre-Meneses, 2015). Classic security and safety problems, such as ensuring the reliability of hardware and protection from natural phenomena, modern systems are so interconnected that security threats from malicious adversaries must be carefully considered (Alves & Morris, 2018). Cybersecurity issues are becoming more prevalent; as such, monitoring and securing systems from cyber breaches, and malicious threats are increasingly critical and challenging (Kesan & Hayes, 2017). Organizations can use the RAA to provide a robust foundation that will potentially serve as an integrated approach to cybersecurity (Leukfeldt & Yar, 2016). Onwubiko (2017) suggested that businesses can implement a protective process by introducing data security solutions to improve data security awareness while reducing cybersecurity threats.

The holistic system approach can be applied when analyzing and implementing cybersecurity strategies. By understanding the root of a breach, small business leaders can support and tighten the disintegrated parts of the target system to prevent future data breaches (King et al., 2018). A shared functionality formed the process used to identify the different system functions. We can view systems through this lens as an interlinked and nested with other systems. In such a method, the analysis may occur at multiple levels about the externalities outside of the system. Chalvatzis, Karras, and

Papademetriou (2019) described small and medium-sized enterprises as systems that consist of diverse components, of which one component is data security. Due to the rise of cyber attacks, cybersecurity is a critical system component for all businesses.

Owners of small businesses can monitor their environment by collecting information about environmental deviations to formulate it as input, which can also be a form of feedback that formed the change or create a cybersecurity strategy (Rothrock, Kaplan, & Van, 2018). The most critical information can formulate a negative input; when there is a breach in the system, the analyzed information can alert the business that a problem needs correction (Marti, 2015). Positive input alerts the business when something is right and indicates the need to continue modifying the activity (Gajic et al., 2015). Small business leaders should analyze and process this information in order to formulate solutions to their cybersecurity needs (Bagschik, Stolte, & Maurer, 2017). An open system is a process used to respond and adjust environmental changes through the input of information. These adjustments can sometimes affect organizational processes (Rothrock et al., 2018). These adjustments may reduce, increase, or support environmental change deviations (Marti, 2015). The organization can analyze information in the throughput to tailor their process to fit their goals (Rothrock et al., 2018). When small businesses adapt to cybersecurity changes, their actions and messages represent the output, and these outputs formed the process used to measure the effectiveness (Jenab & Moslehpour, 2016).

In recent years, researchers have placed a vast amount of resources and effort toward improving and expanding cybersecurity; however, there has been a lack of

significant progress in this field (Joo & Hovav, 2016). While technological improvements resulting from developed security techniques are becoming outdated (Schabacker, Levy, Evans, Fowler, & Dickey, 2019), practitioners created many security techniques years ago when systems were mainly composed of electro-mechanical components and were less complicated than today's intensive systems (Joo & Hovav, 2016). Marti (2015) found that throughput feedback creates new changes in a system, but if the messages and actions are not sufficient, the process repeats until it found a proper solution. If a small business is unable to adopt a cybersecurity strategy variation, then it will ultimately cease to exist. Jenab and Moslehpour (2016) noted that systems theory could be useful in understanding the feedback derived from cyber breaches and creating consistent cybersecurity strategies based on information from the throughput stage. When investigating a breach in a system, it is necessary to understand the relationships between the elements of the environment and the system, as well as the impact's effect on the environment, in formulating the estimated effect of the impact on the system (Naudet, Mayer, & Feltus, 2016).

Leukfeldt and Yar (2016) explained that the RAA could be used to reflect the differences and similarities between offline and online behavior patterns involved in cybercrimes. Researchers found that they could apply RAA to different online cybercrimes by evaluating the patterns of data and crime victimization (Leukfeldt & Yar, 2016). Through a comparison, Reyns (2015) found that the core elements of RAA formed the process used to review and test criminogenic terms in an online environment, with the scheme of criminal behavior represented by motivated offenders and with a proper target

lacking capable guardians. Online-motivated offenders take the form of hackers, fraudsters, stalkers, pirates, and other criminals (Reyns, 2015). Online targets that are suitable for predation include proprietary business data, personal data, and online payment systems, along with vulnerable computer systems that may be disrupted and compromised by unauthorized interference and intrusion (Reyns, 2015). Capable guardians include the various forms of cybersecurity, computerized protections, management access systems, ID authentication, firewalls, virtual private networks, and anti-intrusion and virus software (Van de Weijer & Leukfeldt, 2017).

The impact of inadequate cybersecurity on the possibility of insider victimization could be analyzed using the RAA. Several applications point to the significant effect of routine activity in analyzing cybercrimes (Leukfeldt & Yar, 2016). Balan et al. (2017) observed that cybercriminals continue to probe and target businesses of all sizes with the smallest possible flaws in their systems. These criminals are persistent, well-funded, and sophisticated. Protecting customers and business data is an organizational problem, not just an IT department issue. Tisdale (2015) suggested various viewpoints on a holistic approach to cybersecurity. Owners of small businesses could consider that holistic approaches have their foundation in systems theory. Thus, owners need to understand all the potential entry points for cyber attackers in order to create a holistic cybersecurity strategy that leaves no entry point (Tisdale, 2015).

A holistic cybersecurity approach must accommodate all facets of incident preparedness, customer data security, legal counsel, and regulation for the future (Naudet et al., 2016). Owners of small businesses who adopt an inclusive approach to

cybersecurity are readily able to successfully mitigate, prevent, and remediate cyber attacks (Opitz, 2018). These inclusive approaches must incorporate technology, people, and processes. Owners of small businesses adopting the inclusive approach would consider not only technical factors, but also governance, social, human, and cultural factors. This approach formed the process used to detect and prevent cyber-vulnerabilities (King et al., 2018). It is possible to achieve a robust cybersecurity posture through a combination of integrated security solutions, multi-layer protection, and end-user education (Kafol & Bregar, 2017).

Cybersecurity Threats

Izuakor (2016) concluded that cybersecurity threats are a current reality, and cybercriminals are employing a growing number of tactics to compromise and steal data. Successful cyber attacks could negatively impact the wellbeing of business and economic security (Izuakor, 2016). Janakiraman et al. (2018) concluded that cyberattacks could occur to a business irrespective of the type or size of business. The cause of cyberattacks can by directed through targeted attacks, malicious insiders, and benevolent insiders; as such, owners of small businesses ought to integrate data security plans into their overall processes to reduce the impact of cyberattacks (Janakiraman et al., 2018). Cyber threats describe potential harm, which may come in many forms, including viruses, Trojan horses, phishing attacks, malware, or ransomware network backdoors (Janakiraman et al., 2018). The number of small businesses that are potentially affected, and the damage resulting from these attacks, are at unprecedented levels (Trappe & Straub, 2018). Astani and Ready (2016) cited various estimates of the cost of damages caused by cyber

breaches, which indicates that cyber breaches cost billions of dollars. Kesan and Hayes (2017) found that cyber attacks on the global economy have resulted in losses of $445 billion per year. While cyber attacks on small businesses have increased, the average cost to clean up after a single attack is about $690,000 (Watad et al., 2018).

Cybercriminals are becoming more sophisticated because they found new ways of penetrating security measures, the most common cybersecurity threats facing owners of small businesses are distributed denial of service attack (DDoS), vulnerabilities, spam, phishing, and malware attacks. Malware attacks formulate a process used to steal sensitive customer data when it takes over a website and spread more malware, which could be a devastating effect on small business e-commerce. Iovan and Iovan (2016) concluded that businesses are experiencing a continuous increase in malware threats making it a dynamic continuous challenge.

Most phishing attacks are targeting small business employees; the process is when an attacker impersonates a CEO, manager, a business partner, or a contractor by sending an email with a malware attached when the employee opens the attachment, they would unknowingly installed malware on their computer (Huang et al., 2018). Hennig (2018) pointed out that new phishing sites created every month have increased to an average of 1.4 million. Attackers do this by creating fake web pages that mimic corporate web pages (e.g., Google, Dropbox, Chase Bank, and PayPal). Williams, Bengert, and Ward-Caldwell (2016) reported in their research that the 2014 breach at Sony started with a series of phishing attacks targeting Sony employees. Sony incident proves how the nature of cyber attack has permitted the attacker to leave obscure disinformation and

problematic attribute (Williams et al., 2016). The phishing emails are designed to persuade employees to download the email with malicious attachments or visit counterfeit websites that would install malware into their systems (Goode et al., 2017). The counterfeit websites created by cybercriminals may last up to 8 hours before they create a different site, making it difficult for automated security tools to mark the site as malicious (Hennig, 2018). Attackers are becoming more experienced in hiding behind domains, obscuring their exact URLs, importing more destructive payloads, and misleading users with fake websites (Huang et al., 2018). Simultaneously, the volume of spam and malware attacks has substantially increased in recent years. With the rising rate of small businesses adopting web technology, more systems are vulnerable to malware infections that can exploit and corrupt data. In addition to malware threats, ransomware is a new threat that hackers use to encrypt data stored on the victims' system and lockout users from their system (Goldsborough, 2016).

In the last three years of 2018, the use of ransomware has become a leading method by which hackers are targeting small businesses (Thomas & Galligher, 2018). Brewer (2016) described ransomware software as a malicious attack that allowed hackers to gain access to a company or an individual's vital data. Hackers then hold these data and demand payment before lifting the restriction. In 2016, the primary targets of ransomware were hospitals and end-users (Goldsborough, 2016). The FBI estimated that in 2016 the losses due to ransomware attacks totaled $1 billion (Brewer, 2016). The most commonly used ransomware restriction is to encrypt essential data, thereby allowing the attacker to hold the system or data hostage (Thomas & Galligher, 2018). Hackers then

demand payment before undoing the changes or returning the data. This ultimatum may arrive through on the infected computer as pop-up windows with instructions (Ali, 2017; Richardson & North, 2017).

Some owners of small businesses are less careful about security and controls than end users, which makes even security-savvy customers easy targets. Owners of small businesses often underestimate their risk level and fail to invest in cybersecurity measures; as such, they have become a more frequent target (Goldsborough, 2016). Sultan, Khalique, Alam, and Tanweer, (2018) stated that since the first ransomware attacks occurred in the mid-2000s, there have been over 7,600 attacks (FBI, 2015). In 2015, the IC3 received over 2,453, complaints of ransomware that cost over $1.6 million (FBI, 2015). In 2016, the IC3 received 2,673 complaints identified as ransomware, represented a loss of over $2.4 million (FBI, 2016b).

Hackers that formerly focused on blanket attacks have increased their presence (Sandberg, 2019). Their new method involves targeting specific businesses, consumers, and hospitals with a critical need for data (Yaqoob et al., 2017). Consumers are becoming the most likely victims of ransomware, as some businesses are unable to recover from the loss of data because the cost of recovery is prohibitive (Ali, 2017). The use of mobile devices and social media with relatively lax security has made organizations—particularly especially those that utilize social media for recruitment and marketing are vulnerable to attackers (Sandberg, 2019). Social media enables unprecedented access to individual and business data, which is another weak access point that owners of small businesses must learn to control (Kaushik, Kumar Jain, & Kumar Singh, 2018). Hackers

also exploit security weaknesses in the operating systems, firmware, encryption software, and productivity software that are used by small businesses (Kesan & Hayes, 2017). Various areas of technology are vulnerable to cybersecurity threats. Cyber threats to small businesses have become a daunting problem because hackers are after business and customer data. These businesses do not have multi-million-dollar security budgets, and therefore are a much easier target (Krunal & Viral, 2017).

Other areas of interest to researchers are security weaknesses associated with e-commerce systems, as well as the methods owners of small businesses used to protect data (Burhan, Rehman, Khan, & Kim, 2018). In a small business survey, the researchers found that most owners of small businesses outsource their electronic commerce websites (Choras & Kozik, 2015). Although this may have a significant impact on solving the physical problem after being outsourced, the IP address that the business server used to host the site can remain visible through a basic search via Google (Sharma & Lijuan, 2015). Web application attacks are the most single predominant and devastating security threat that most businesses are facing today (Sobitha Ahila & Shunmuganathan, 2016).

Owners of small businesses need to adopt a robust cybersecurity system with multifaceted and integrated security solutions (Pan, White, & Sun, 2016). Owners of small businesses need a comprehensive security plan that would address a wide variety of vulnerabilities and Internet-based attacks. This comprehensive security plan could also be modified to periodically tackle the constant changes in Internet-based attacks (Sabillon, Cavaller, Cano, & Serra-Ruiz, 2016).

Holistic Cybersecurity Strategies

Cybersecurity is a proactive approach that could be used to protect Internet-linked systems, including software, hardware, and data, from cyber attacks (Trappe & Straub, 2018). From this viewpoint, cybersecurity is connected to an organization's practices, policies, and physical infrastructure (De Oliveira Albuquerque, Garcia Villalba, Sandoval Orozco, De Sousa Junior, & Kim, 2016). Cybersecurity is considered a significant challenge for any organization that must deal with cyber threats (De Oliveira Albuquerque et al., 2016).

A holistic cybersecurity strategy covers the preparations and precautions against cyber breaches (Ceric, 2016). Holistic cybersecurity strategies include corrective and preventive measures that some owners of small businesses used to protect confidential company data from cyber attacks (Allodi & Massacci, 2017). A cybersecurity strategy is an essential technology element that organizations are using to protect their system from an imminent attack. Good cybersecurity practice ensures the integrity, confidentiality, and availability of data security (Elifoglu, Abel, & Tasseven, 2018). By becoming proactive in cybersecurity issues, owners of small businesses are essentially safeguarding their organization’s security system.

Watad et al. (2018) noted that adopting information security tools is not consistent across all small businesses. These are due to inconsistency, lack of information security awareness, and the lack of necessary skills and knowledge to select and implement security solutions (Watad et al., 2018). These factors made it difficult for small businesses to implement a consistent, proactive cybersecurity strategy. Small businesses’

information security strategies should be able to address the continual growth of cyber threats and risks. However, to be effective, owners of small businesses must align strategies closely with business goals (Nastasiu, 2016). Owners of small businesses need to determine the level of their system vulnerability and develop a suitable holistic plan to address vulnerabilities (Jones & Shashidhar, 2017). Some owners of small businesses have incorporated holistic strategies that can detect, protect, and respond to current cyber attacks.

The holistic approach incorporates human, technical, and physical factors relevant to detecting, preventing, and correcting current cybersecurity vulnerabilities (Kafol & Bregar, 2017). Some owners of small businesses are defending against cybersecurity attacks by installing system security, security awareness, education, training employees, and intrusion detection to prevent targeted attacks (Almeida, Carvalho, & Cruz, 2018).

System Security Strategy

Some owners of small businesses have installed computer protection like firewalls, antivirus software, intrusion detection systems, two-factor authentication, phishing filters, and many other security products to combat Internet-based attacks (Huang et al., 2018). Firewalls are a vital strategy for small business network security, as they are a set of related layers against threats and prevent outsiders from accessing data on the business network as described by Elifoglu et al., 2018. Internal firewalls are being used to fortify the computer system by some owners of small businesses. Firewalls could be used to prevent pop-ups, cookies, malware, and e-mail viruses from infecting the business network (Elifoglu et al., 2018).

Some small businesses are contacting security companies for antivirus, anti-malware, and anti-spyware software solutions that can protect their computer system from cyber attacks (Huang et al., 2018). Some small businesses' computers are secured with antivirus, anti-malware, and anti-spyware software that have been configured to receive the regular update.

Intrusion Detection Strategy

Some owners of small businesses that have the resources to implement intrusion detection are adopting a defense-in-depth (DID) strategy to protect valuable data and information (Rahman et al., 2019). The implementation of a DID strategy gives them the ability to detect, defend, and mitigate various types of cyber attacks. This robust security measure combines a series of different defensive mechanisms; such that, if one fails, another is immediately in place to thwart the attack, For example, some businesses include automated vulnerability testing of both the website and the system that supports it (Burgess, 2016). Security testing is part of all stages of the system's life cycle and is a practical solution used to secure business data from attacks (Wolff, 2016).

DID strategy require that relationships between network resources and network users be scalable so that controlling access could go beyond placing firewalls between segments on the network. Wolff (2016) noted that DID strategy would require a tailored strategic approach that could be applied to various levels of security to restrict setting and protect critical assets, such as proprietary and confidential information. The DID strategy also provides a series of defense that includes malware scanners, firewalls, intrusion detection systems, and local storage encryption tools (Rahman et al., 2019). Owners of

small businesses could deploy these strategies to close gaps in their security system and protect their businesses from an attack.

Cyber Security Awareness Education and Training

Hadlington (2017) noted that understanding what governs good cybersecurity practices is the need to focus on awareness and employee training. Employee education has gone a long way to helping some owners of small businesses to detect and ward off cyber attacks. Employees are trained to understand cyber attacks warning signs, safety, and the proper methods to respond to an attack, understanding their duties and responsibilities, the procedures and processes needed to protect confidential company data from cyber attacks (Hadlington, 2017). Some owners of small businesses are educating their employees about the various online threats, including the safe use of social networking sites (Elifoglu et al., 2018). The first line of defense against a data breach is often the employees. Having employees who understand their responsibility in handling data goes a long way towards preventing a breach before it begins.

Janakiraman et al. (2018) wrote that businesses are developing adequate security awareness through employee training scenarios. Some owners of small businesses have also implemented a cybersecurity awareness program that ensures employees are cognizant of the significance of protecting sensitive information and the risks of mishandling information (Williams et al., 2016). Conteh and Schmick (2016) noted that new employees must be required to attend preliminary training during orientation. The training would help to build awareness by exposing new employees to various cyber-threats and the tactics and behaviors used by hackers. Some owners of small businesses

have cybersecurity policies on the importance of securing information, defining risk management, listing the types of information that ought to be secured, and identifying various threats using best practices (Rizov, 2018).

A culture of security awareness helps owners of small businesses prepare against cyber-incidents. An atmosphere of this kind includes reporting, responsiveness, and openness that allows quick responses to potential threats and mitigates the issue (Tasevski, 2016). Information security awareness training is essential because it does not merely educate employees on possible security threats and the steps to prevent them but also focuses on organizational culture on security awareness (Muronga, Herselman, Botha, & Da Veiga, 2019).

Outsourcing Strategy

Some owners of small businesses need to be able to defend against and limit cyber attacks, when it comes to cybersecurity and defensive capabilities, the needs of small businesses are similar to those of larger organizations. The main difference is that some owners of small businesses are using standardized cloud services, for example, Microsoft Office 365, SaaS, Cloud Infrastructure, and Google Docs instead of customized applications and infrastructure (Mokwena & Hlebela, 2018). Also, they are outsourcing their cybersecurity to the right technical partner or service provider that can handle their day-to-day security processes and also secure critical assets, such as proprietary and confidential information (Prince, 2018). Ogunshile (2018) concluded that having the right cybersecurity partner to manage their security environment would take an enormous burden from owners of small businesses. While working with vendors,

some owners of small businesses have developed some security measures to protect sensitive data. Some owners of small businesses still lack adequate response to an attack because they do not have the means and techniques to properly manage cyberattacks (Makridis & Dean, 2018).

Owners of small businesses must be able to manage and protect both business' and customers'data by using multiple vendors to make data-driven decisions (Kim, Lee, & Ryu, 2018). Some owners have taken proper steps to invest and implement defense systems using different approaches, such as defending their system from a specific set of attacks or limiting data access (Williams et al., 2016). These steps could ensure that they can quickly detect and respond to them before data are stolen (Vlad-Mihai, 2017). Other owners of small businesses prioritized what they protect. They plan to spend on technological platforms because their needs are the same, even though the scale of their expenditure is less than a larger organization (Kim et al., 2018). The problem facing owners of small businesses is often intractable; unlike big organizations, small businesses are not able to invest in the necessary resources and people to manage IT security (Rothrock et al., 2018).

Those owners of small businesses who are not able to afford defensive cybersecurity systems are moving their technology to the cloud system because of its affordability and unmatched utility (Korte, 2017). A cloud service agreement is accompanied by security services that include an understanding of how the business collects data, usability, and ownership. These services have helped some owners of small

businesses to prevent data losses, which have the potential to jeopardize business reputation with customers, suppliers, and partners (Mokwena & Hlebela, 2018).

The general trend is for owners of small businesses to depend on cloud vendors to provide more and more e-commerce services. As technology improved, more and more product is being delivered through the cloud system with the democratization of cybersecurity (Pantangi, Xiong, & Makati, 2016).

Third-Party Vendors Strategy

Some owners of small businesses that are unable to invest in cybersecurity are either retaining managed security services providers (MSSPs) or relying on specialized IT vendors (Cezar, Cavusoglu, & Raghunathan, 2017). They developed an effective cybersecurity strategy by outsourcing their information security to an MSSP that helped them gain access to professionals who monitor and maintain their systems remotely to ensure privacy and security best practices (Lopes & Oliveira, 2016).

Owners of small businesses face many IT challenges, but by outsourcing their information security, everything from website functionality and cloud migration to technology update and data backups (Njenga & Jordaan, 2016). Outsourcing services include business continuity, operational efficiency, maximum return on technology investments, cost reductions, as well as better protection for business and customer data (Li, Liu, Belitski, Ghobadian, & O'Regan, 2016). These measures have supports and resources that can handle current cybersecurity challenges and protect against cybercrime as well as disaster recovery processing should an attack occur (Opitz, 2018).

A Holistic Prevention Strategy

Cyber-terrorism has become a more significant threat because owners of small businesses who are government contractors often become the target of malicious attacks (Wainwright, 2018). The alarming rise of such incidents has made cybersecurity a significant concern, and researchers called for creating a cyber-terrorism framework (Terzi, 2019). Besliu (2017) stated that the highest risk of cyber attacks is government employees, followed by business employees with access to government networks. These risks have become a significant concern to owners of small businesses because some receive government and large corporate contracts. Without standardized preventive methods capable of adapting to current threats, cyber-terrorism will increase as a threat to small businesses (Albahar, 2017).

A holistic prevention strategy could be used to avoid the effects of cyber-terrorism. Kadir, Judhariksawan, and Maskun (2019) concluded that deterrent strategies are not adequate to prevent cyber-terrorism because deterring all unwanted cyber-threats has proven difficulties. Business leaders need a realistic expectation for deterrence that would be able to minimize and mitigate the impact of cyber-terrorism (Wainwright, 2018). The greatest danger to cybersecurity for small businesses comes from trusting providers, strategic partners, and allies who have not been engaged in prevention and detection (Nicola, 2018). As a result, some owners of small businesses are using a preventive strategy that is not well-defined and may not defend against cyber-terrorism (Nicola, 2018). Gross, Canetti, and Vashdi (2017) noted that resilience efforts constitute securing the bridge between the system that supports business operations, upgrading

network hardware, and Internet connectivity pathways to improve situations following a widespread and potentially devastating cyber attack. Significant preparations would also help improve cyber-resilience that can manage and control the aftereffects of a cyber attack (Kadir et al., 2019).

Data Protection Strategy

Data storage is another growing concern for small businesses. The way that data is shared and stored evolves with the advance of technology. The Internet of Things (IoT) refers to Internet-connected devices that collect and share data (Riahi Sfar, Natalizio, Challal, & Chtourou, 2018). The IoT is helping owners of small businesses streamline their processes and compete with other businesses to reach millions of customers around the globe (Janecek, 2018; Makridis & Dean, 2018); However, this also can lead to cyber breaches. Owners of small businesses need to guarantee that IoT devices are connected correctly and that there is no room for a data breach, as these devices are susceptible to the same Internet-based attacks as businesses (Riahi Sfar et al., 2018).

The IoT shares data through Internet protocol with other communication devices that are equipped with sensors, microchips, and actuators to help prevent a breach (Gil, Ferrandez, Mora-Mora, & Peral, 2016). Some owners of small businesses use this technology to improve their everyday work through advancements, such as free smart office assistants (Ban, Choi, & Kang, 2016). Small businesses are prone to cyber attacks through these connected devices because cybercriminals are aware of the different Internet protocols (Stanciu, & Tinca, 2017). Guitton (2017) recommended three strategies to secure against Internet-based attacks: (a) prevention before an attack, (b) detection

during an attack, and (c) response after an attack. Early detection and immediate mitigation of cyber attacks are the hallmarks of managing Internet-based services and having a proactive defense strategy against such threats (Anderson, Baskerville, & Kaul, (2017).

Some owners of small businesses applied these strategies to secure Internet-based systems: monitoring security against cyber attacks, studying the effects of cyber attacks on their system by developing an attack tree by generating intrusion scenarios to explore specific attack paths (Guitton, 2017). Financial organizations are more prepared to handle a data breach attack because they developed a better monitoring system, as they could detect and prevent breaches. Developing a monitoring system and data protection strategies is essential to small business operations, regardless of the type of connection the business is using to send data (Munier & Kemball-Cook, 2019).

Kesan and Hayes (2017) indicated that more than 63% of customer credit card data are unencrypted when stored in the server, and 7% of businesses still keep records of data contained in the card's magnetic bar. These practices magnify the business' security vulnerabilities (Kesan & Hayes, 2017); there are alternative methods to safeguard customer credit card information during transmission as some owners of small businesses have strengthened their payment gateway with banks that issue cards; this has helped to secure credit and debit card information during purchases (Greenacre, 2015). Banks that issue a credit card to small businesses are supplying tools that the owners use to confirm card payments and ensure that customers' data are safe (Greenacre, 2015). Some owners of small businesses are practicing isolation, which is one of the best cybersecurity

practices for credit and debit cards (Greenacre, 2015). These are done by isolating payment systems on a separate computer from the regular network, which has helped to limit the risk and impact of attacks (Awrey & Van Zwieten, 2018).

Some owners of small businesses updated their payments processor and all point-of-sale (POS) systems that include mPOS devices with updated cybersecurity technologies (Awrey & Van Zwieten, 2018). Encrypted card data could be manipulated so that each legible entry would be read-only as a string of obscure characters if an unauthorized user accessed it (Cox & Pilbauer, 2018). By using tokenization, the payment processor could securely store card data (Awrey & Van Zwieten, 2018). Some owners of small businesses also took advantage of e-commerce websites that offer built-in security systems with payment processing services that would protect their online customers' data (Holland & Gutierrez-Leefmans, 2018).

Owners of small businesses could also identify various potential internal and external data security risks and develop a counter-attack strategy to protect against them (Wadhwa & Arora, 2017). Some owners of small businesses have designed and implemented security plans, data privacy, policies, and procedures that include incident response and crisis management plans (Tisdale, 2015). These also include potential shareholders, liability issues, regulatory interests, a data retention policy, and ways to dispose of unwanted information (Almeida et al., 2018).

Data Breaches

Janakiraman et al. (2018) described data breach as the inadvertent or intentional exposure of confidential data to unauthorized parties. Data breached occur when hackers

gain access to private data such as social security numbers, addresses, passwords, phone numbers, and usernames from breached sites such as credit bureaus, retail stores, and email providers. A data breach could occur for various reasons, including fraud, theft, and human error (Janakiraman et al., 2018). Among the data breaches that have taken place in the United States and globally included retail brands like Target lost over 40 million customers data, Home Depot over 56 million customers data, Michaels over 2.6 million customers data, Neiman Marcus over 1.1 million customers' data, and Staples over 1.2 million customers were hacked (Kim, Johnson, & Park, 2017). These retailers are the major suppliers to small businesses, and these massive data breaches are directly affecting small businesses, which are resulting in millions of compromised consumer accounts (Plachkinova & Maurer, 2018).

Selznick and Lamacchia (2018) concluded that during the past five years, the number of cyber attacks on organizations with 250 or fewer employees increased dramatically. In 2015, the average cost of a data breach was $6.53 million, making this a significant problem for organizations (Selznick & Lamacchia, 2018). In 2017, the Chipotle Mexican Grill restaurant chain was a target of cybersecurity attacks. The breach affected 2,250 restaurants nationwide (Selznick & Lamacchia, 2018). The hack was due to malware designed to access payment card data from cards used at POS devices in certain restaurants (Selznick & Lamacchia, 2018). In 2016, Newkirk Products, a small business service provider that issues insurance healthcare ID cards for Blue Cross and Blue Shield, reported a breach on the server that holds member information, and some data were stolen (Selznick & Lamacchia, 2018).

Data breaches could be a result of an accidental data breach or an attack; objectives include competitive data used for corporate espionage purposes, employees' social security numbers, financial, medical records, and customers' records (Brown, 2016). The fallout of such breaches could persist for years, as was the case in the Equifax attack (Moore, 2017). Bai, Jiang, and Flasher (2017) noted that in 2016, the medical and healthcare sector experienced 34.4 % of the 185 data breaches to date. The number of records exposed in these breaches totaled nearly 4.5 million, representing about 34.4 % percent of the total as of July 2016 (Bai et al., 2017). 90% of small businesses that experienced data breaches were unaware of the breach until informed by a third party, as cybercriminals continue to adopt new techniques as their threat continues to advance (Eddolls, 2016). Owners of small businesses must become proactive by being aware of these changes and ensuring that their business process is adequately prepared and protected.

Data Breach Prevention Strategy

Owners of small businesses could develop resilience in combating future cyber attacks by creating a cyber-defense strategy that could position them to dynamically respond to attacks through improved situational awareness, active command control, and active defenses. These approaches would provide a proactive response to cyber attacks, as recommended by Williams et al. (2016). Previous organizational methods of handling data breaches include implementing an incident response plan after the breach (Fisher, Norman, & Klett, 2017). Owners of small businesses generally employ reactive strategies

to combat data breaches rather than proactive approaches (Galinec, Moznik, & Guberina, 2017).

A proactive approach for data breaches would incorporate layered security strategy to detect suspicious activity before a breach occurs and put a stop to a potential breach as early as possible (Williams et al., 2016). Most scholars studying cybersecurity-focused on the technical aspects of a data breach incident, which is useful in helping organizations understand how a breach occurred (Parks & Adams, 2016). Owners of small businesses could then create internal assessment procedures for determining effective security control. Some owners of small businesses are creating a catalog of security controls to meet current cybersecurity needs that could also apply to the future (Brown, 2016). Allodi and Massacci (2017) provided steps that can be applied to specific areas where businesses could improve their cybersecurity strategy. These can be done not by investing in the latest technology but by improving internal organizational processes.

Data Leak Prevention Strategy

Data leakage is another issue that poses threats to organization operations, financial losses, and reputational damage. Losing sensitive information could be detrimental to the long-term growth and stability of small businesses (Cheng, Liu, & Yao, 2017). While data leaks could be considered a minor inconvenience, the reality is that the worst data breaches occur over time by devious means, which have far-reaching consequences when confidential data fall into the hands of an unauthorized user (Alneyadi, Sithirasenan, & Muthukkumarasamy, 2016).

Data leakages can be caused either by malicious intent or an inadvertent mistake by an insider. In either case, exposure of sensitive information can severely hurt an organization (Angst, Block, D'Arcy, & Kelley, 2017). The potential damage and adverse consequences of a data leak incident can be classified into the following two categories: direct and indirect loss. Direct loss refers to physical damage that is easy to measure and estimate quantitatively. The indirect loss is much harder to quantify and has a much broader impact regarding cost, place, and time (Rothrock et al., 2018).

The scope for data leakage is pervasive and is not limited to just web and email; data leakage includes the unauthorized transmission of data to an external destination from within an organization, which can either be intentional or inadvertent (Vavilis et al., 2016). A combination of factors like insider or outsider threats can cause a data breach; from a targeted attack, which is often inadvertently allowed by well-meaning insiders who do not follow data or security policies (Choi, Kim, & Jiang, 2016). Data leakage can either be created intentional or unintentional; Intentional leaks occur when data are purposely transmitted to someone outside the company, who does not have a legal right to possess the information (Angst et al., 2017).

The potential damage and adverse consequences of a data leak incident can be classified into two categories: direct or indirect loss. Direct loss refers to physical damage that is easy to estimate, and indirect loss is much harder to quantify that has a wide-ranging impact that includes cost, place, and time (Rothrock et al., 2018). The scope for data leaks are pervasive and not limited to just the web and email; data leakage includes the unauthorized transmission of data to an external destination from within an

organization, intentionally or inadvertently (Vavilis et al., 2016). A combination of factors (such as insider or outsider threats) could cause a data breach. A targeted attack is often inadvertently allowed by innocent insiders who do not follow security policies (Choi et al., 2016).

In most cases, careless insiders without a motive or intent to cause harm could leak data and cause a situation that can be just as bad as one caused by malicious attackers (Dhawase, Chaudhari, Kolambe, & Masare, 2018). Employees are the most common security threat to most organizations; when they abuse their access, they harm security layers of the company and may cause considerable losses (Hennig, 2018). In 2014, eBay asked their 145 million users to change their account passwords due to a breach that affected personal information and encrypted passwords (Williams et al., 2016). Hackers gained access to an eBay account through stolen login credentials from eBay employees. Organizations must perform consistent vulnerability assessments on both internal and external network systems (Williams et al., 2016). Owners of small businesses need a breach response plan that would trigger quick responses to data breaches to decrease the impact. The plan could contain steps that involved notifying the appropriate personnel and vendors who could contain the breach. Kim et al. (2017) pointed out that in a crisis, businesses that are faced with data breaches should avoid legal consequences by disclosing the nature of the breach to affected and potentially affected customers whose data may have been compromised.

Data leakage requires protective measures to mitigate future threats. Data loss prevention (DLP) is a strategy that ensures users are not able to send confidential

information outside a company's network (Costante, Fauri, Etalle, den Hartog, & Zannone, 2016). These strategies involve a combination of user security policies and tools. Owners of small businesses need a data protection policy that includes information security, privacy, and need that relate to the business. Kaur, Gupta, and Singh (2017) noted that DLP could be used to reduce risk, improve data management practices, and even lower compliance costs. DLP increases user awareness by alerting them when there is a suspicious email; this has helped to increase business' responsibility and used to correct oversights to security policy before a leak happens (Ma, 2017). Owners of small businesses can use DLP to improve processes, identify steps to uncover security flaws, and implement remediation actions.

Summary and Transition

Summary

The literature supports the intent and problem statement of the current study. Cybersecurity is a relatively new field, with a limited number of extensive studies and models. As technology continues to evolve, cybersecurity will become a viable field of study due to the pressing need to secure data in all settings. The growth of cyber-dominance makes cybersecurity a pressing need (Jia, Qi, Shang, Jiang, & Li, 2018).

While all businesses are vulnerable to cyber attacks, it is clear that small business is more susceptible to cyber attacks than large organizations. However, it is also clear that owners of small businesses do not have access to resources and techniques like large organizations. Larger establishments typically have a robust defense system that is difficult to compromise or breach. Many larger organizations' systems are interconnected

with those of small ones. When hackers compromise the security system of small or mid-size businesses, they can then easily penetrate the defenses of even multinational corporations. Hackers are aware of complacency among small businesses concerning cybersecurity. Hackers understand that owners of small businesses invest relatively little money to improve the state of their cybersecurity; this weakness is being exploited and making small businesses vulnerable to attack. In short, existing researchers studying cybersecurity breaches have predominantly focused on the impact of public disclosure of such incidents on the affected organizations' market valuation. Chen (2019) examined the impact of data breaches on consumers and ways at which owners of small businesses can reduce the impact of data breached. The author further indicated that owners of small businesses should be able to provide insights on how to prevent and manage data breaches. The impact and cost associated with a single breach can be catastrophic to small businesses. It is necessary to address the different factors that influence owners of small businesses that lack cyber-defense strategies. In this literature review, I substantiated the need for owners of small businesses to be aware of cybersecurity threats, as well as develop preventative strategies to combat security threats and eliminate privacy concerns.

Transition

In Section 1, I included information to support the research problem. Additionally, I presented the background that supported the phenomenon that some owners of small businesses lack the knowledge of cyber-defense strategies to protect business data from cyber attacks. In the problem statement, I addressed both the general

and specific business problems, while the purpose statement contained the justification for the research method, design, and participant size. Using a detailed literature review, I supported the research problem. In Section 2 of this study, I deliberate on the research framework components, which includes further details on the overall intent of the study, participant enlistment, data collection, and analysis. In Section 3 of this study, I provide a formal presentation of the findings of the study.

Section 2: The Project

Purpose Statement

The purpose of this qualitative multiple case study was to explore strategies owners of small businesses use to protect confidential company data from cyber attacks. The target population for this study consisted of five successful owners of small businesses in the Fort Lauderdale, Florida area who have implemented effective cybersecurity strategies to protect their business data from cyber attacks. The implications for positive social change include the potential to enhance sound cyber policies that can be used to protect business and customer data, thereby increasing customers' confidence, increasing businesses' economic growth, and stimulating the socioeconomic lifecycle, resulting in potential employment gains for residents in communities.

Role of the Researcher

My role as a researcher involved selecting participants, preparing the interview questions, collecting and recording data in an accurate manner as it relates to the study problem statement as described by Bansal, Smith, and Vaara (2018). Researchers who use qualitative methodologies must develop sufficient knowledge to comprehend why it is essential to interpret and understand the data needed to conduct the research study (Cumyn, Ouellet, Cote, Francoeur, & St-Onge, 2018). Scholars who used qualitative methodologies must successfully develop their skills with research instruments that could be used to collect data (Yin, 2018). Researchers who used qualitative methods must develop, conduct, and interpret comprehensive qualitative data analysis that could be

used to present study findings while following basic ethical standards (Bansal et al., 2018). Researchers must adhere to basic guidelines and ethical principles that would assist in resolving ethical problems. I enacted protocols to ensure that participants were treated with the highest ethical standards, as described in the study conducted by Miracle (2016). I reviewed and observed the basic ethical principles detailed in the *Belmont Report*. To be able to follow this objective, I completed the Collaborative Institutional Training (CITI) course training (Certification Number: 8042684). The *Belmont Report* served as the ethical framework for this research because it outlines a framework that guarantees respect, beneficence, and justice for participants (DHEW, 1979). Compliance with these guiding values ensured that I conducted my research using an ethical foundation. I adhered to ethical principles and guidelines by applying the three principles to minimize risks and ensure benefits to participants (see Miracle, 2016). I maintained ethical and professional relationships with participants, as described by Cypress (2018). The selected owners of small businesses are not in my professional or social network. I did not have a professional relationship with the study participants; this helped to ease the concern of participants who were reluctant to participate or hesitate to reveal sensitive information that benefited the study. Amankwaa (2016) pointed out that researchers who plan to create a qualitative proposal should create a trustworthiness protocol. These provided evidence of consistency and accuracy concerning the process of how data were collected and the timeline directing the activity similar to the approach used by Cypress (2018). I prepared my research protocols with a detailed process as to how I collected data in the interview protocol (see Appendix B).

I found that there are no conflicts regarding the boundaries between practice and research on how I collected data from owners of small businesses. Owners of small businesses voluntary participants in this study and have the option to opt-out at any point during the research process. I ensured that participants' experience in cybersecurity matches the goal of the study. I did not include those with too much or too little technical knowledge; only those with the appropriate level of experience were included for the research study. Participants were encouraged to speak openly during the interview process to guarantee that their point-of-view was relevant. I was neutral, as such, avoided impacting how participants are answering the research questions. To further protect participants, I excluded the names of organizations and participants from the study. To assist in maintaining consistency and structure between interviews and ensure that the data collected are accurate and unbiased, I used the interview protocol similar to the approach described by Van Hilten (2018).

I also used member checking to seek feedback from participants to mitigate bias. Member checking is a technique that involves participants validating the interpreted data after the interview, and which could establish credibility with participants (Birt, Scott, Cavers, Campbell, & Walter, 2016). Thomas (2016) described member checking as a method that could be used to obtain participant approval and reduce research bias. Following each interview, I seek feedback from participants, which helped to improve the credibility of the collected data. After participants validated the interpreted data, I used the data to capture the themes for accuracy.

Participants

Recruiting participants is the foundation of an effective research study because research results are only as useful as the participants' involvement. As the researcher and the primary data collection instrument for this study, I used the purposive snowball sampling strategy similar to the approach described by Valerio et al. (2016). These are based on a referral tactic in which I corresponded with some owners of small businesses with specific characteristics that were used to recommend and recruit others with the same characteristics. These tactics were beneficial in recruiting the five successful owners of small businesses in Fort Lauderdale who have implemented effective cybersecurity strategies**.**

Meyvis and Van Osselaer (2017) noted that recruiting participants in research studies is an essential part of the study process. I also recruited participants using business statistics publications provided by local government and state agencies. This strategy helped to optimized participant recruitment and gained access to their professional perspective, similar to the approach used by White and Hind (2015). The first technique of population search consists of business listings from inquiries on the U. S. Small Business Administration (SBA) website for the South Florida District–Miami (SBA, 2018b). Using the SBA website links gave me access to small business datasets that helped in my preliminary source for recruiting participants who met the sample population criteria for this study. Another search technique that I used to recruit participants from the City of Fort Lauderdale was using the city business resources guide, which helped to develop my sample population (City of Fort Lauderdale, 2018; Greater

Fort Lauderdale, 2018). The next technique was accessing owners of small businesses from the Broward County Small Business Assistance Council, whose main aim is to encourage the growth of small businesses in Broward County (SBA, 2018b). Finally, I attended a monthly meeting for the Broward County Economic Development Commission, where I met some owners of small businesses, which help to provide another means for recruiting participants.

Participants were required to meet the established small business size standard as detailed in the *North American Industry Classification System* dated 2012 or later (SBA, 2018a). Peticca-Harris, DeGama, and Elias (2016) stated that researchers must comply with academic institution requirements while organizing and planning their study; this includes obtaining approval from an ethics board. I also contacted participants by phone to establish a working relationship and introduce participants to the study, after I obtained the IRB approval (No. 06-26-19-0490285) from Walden University. I also contacted potential participants in person and in writing to maximize the time spent with each participant, similar to the approach described by Griffith, Morris, and Thakar (2016). After owners of small businesses have indicated their readiness to participate in this research, I asked each one to sign a consent form, which was in the IRB requirements spelled out in Walden University's ethical guidelines. Researchers must build and establish a trusting relationship by keeping the information of participants confidential, as described by Gonzalez-Saldivar et al. (2019). I used the participant consent form to recognize and establish participant privacy and trust in this study.

Research Method and Design

Research Method

I chose to use a qualitative method for this study. Researchers use qualitative methods to understand the underlying phenomena to gain experience (Jacobs & Tschotschel, 2019). Qualitative methodology was appropriate because it was useful in gaining insight into the strategies that owners of small businesses have used to protect company data from cyber attacks. Bansal et al. (2018) indicated that qualitative methodology is most appropriate for studying social phenomena that do not generate sufficient data for quantitative studies. My intent was not to quantify why owners of small businesses do not implement security control, but rather to learn the strategies that owners have used to protect their company's data from cyber attacks. A quantitative research method was unsuitable because I was not examining relationships among variables of cyber security data. Further, mixed methods were inappropriate for this study because this approach involves integrating both qualitative and quantitative components. I was not studying relationships and trends relating to cyber security variables. Also, I did not have access to this type of data to add to the qualitative data from the interviews (see Nelson, 2016). Mixed methodologies involve collecting, analyzing, and integrating both qualitative and quantitative methodologies to solve a research problem (Park & Park, 2016).

Research Design

A multiple case study was the appropriate design choice for this study. Other research designs that were considered included ethnographic, phenomenological,

narrative, and case study. Ethnographic research was unsuitable for this study because it seeks to identify and understand the behaviors and cultural practices of a specific group (Cardoso et al., 2017). The goal of phenomenological research is to provide the meaning of the experiences of a group or an individual that relates to a particular phenomenon (Flynn & Korcuska, 2018). Past experiences did not provide insights into the strategies that were reviewed in this study; therefore, the phenomenological research design was not appropriate. Narrative research provides a visual representation or written stories of participants' personal experiences (Bruce et al., 2016), but was not appropriate for this study because analyzing strategies does not benefit from telling stories from past experiences. The purpose of this study was to analyze strategies used by owners of small businesses to protect confidential data from cyber attacks. The multiple case study design was suitable for this study because it can be used to identify, describe, and understand collected data, as noted by Heale and Twycross (2017).

A single case study set focuses on a specific case, while a multiple case study focuses on multiple cases that allow for a more comprehensive exploration of the research questions and their development (Wilson, 2016). A multiple case study was the most suitable design choice because using multiple case studies allows the researcher to explore phenomena and utilize multiple forms of data collection to gather information on strategies owners of small businesses have used to protect their business data from cyber attacks. I interviewed five successful owners of small businesses for this study to achieve data saturation similar to the approach described by Boddy (2016). When I reached the point in the interview process that the data collected offered no new information (or was

redundant), data saturation was attained as described by Benoot, Hannes, and Bilsen, (2016).

Population and Sampling

The study population was five owners of small businesses in Fort Lauderdale, Florida. Benoot et al. (2016) noted that a qualitative research purposeful sampling is a non-probability sampling method that a researcher uses to identify and select a set of features within a sample as it relates to the phenomenon of interest. Purposeful sampling is beneficial when conducting interviews because it provides a set of recommendations that can be used for multistage designs (Benoot et al., 2016). A purposeful sampling of four participants was drawn from the population of those who have successfully implemented cybersecurity strategies. The purposeful sample participants were derived from face-to-face and semistructured interviews. These semi structured interviews took place at a convenient location to avoid distractions. Benoot et al. (2016) noted that an appropriate sample size for a qualitative study would depend upon the study context. Purposeful sampling was suitable for this study because it allowed me to gain different viewpoints and collect data from participants who were knowledgeable and had implemented effective cybersecurity strategies. Data saturation is significant because it indicates data accuracy, and this can occur when no further categories or themes can be derived from the collected data (Benoot et al., 2016).

For a multiple case study design, I needed at least five interviews to achieve data saturation similar to the approach used by Boddy (2016). If I did not reach data saturation after interviewing the five successful owners of small businesses, I would further conduct

interviews until data saturation is achieved. When I reached the point in the interview process that the data collected offered no new information, I attained data saturation similar to the approach described by Benoot et al. (2016).

Ethical Research

Protecting participants' privacy is a critical factor in this research study. My top priority was maintaining the highest standards of ethics that focused on the highest quality of research. I began the study after obtaining IRB approval (No. 06-26-19-0490285) from Walden University. I avoided falsification, plagiarism, and misconduct, as described by Burkholder and MacEntee (2016). To assist in maintaining moral principles, I observed the following research protocols:

- I only used participants who gave their consent in the data collection process. Participants volunteered by agreeing to contribute to the study by replying "I consent" to the informed consent form that was emailed to participants (see Appendix A). This approach was found to be effective by Gallin, Ognibene, and Johnson (2017).
- Participants had the liberty to withdraw at any point in the research process without penalty by verbally communicating so during the interview, or by contacting me by telephone or email. This approach was used by Soulier (2019). Participants also had the right to express his or her concerns to withdraw from the research process at any time.
- I established identity protection for participants' personal information during their involvement in the study. All personal data collected during the interview are

remaining confidential, following IRB standards.

- Participants were guaranteed protection on all data collected, including individuals' names and company information. A masking process was relevant to preserve participants' privacy and confidentiality. This approach was found to be effective by Korstjens and Moser (2017). Participant names are labeled with a random number, and a random letter was used to represent organization names.
- All original paper copies are scanned and stored in a private cloud account with a protected password, after which copies of the originals paper will be mechanically shredded. All data collected from the date of the interview are stored no longer than 5 years. After 5 years, I will delete all electronic data of the research record from the private cloud account.

Data Collection Instruments

This qualitative multiple case study involves face-to-face, semistructured interviews to collect data. Oltmann (2016) noted that semistructured interviews involve a list of open questions that allow participants to respond to the researcher's interests in a focused way. DeJonckheere and Vaughn (2019) suggested that semistructured interviews help to understand the dynamics of a situation by data collection. I used semistructured interviews to explore strategies that owners of small businesses use to protect confidential company data from cyber attacks. Also, has the primary investigator that conducted the interviews and acted as the data collection instrument, I supplemented my data collection with observational notes, which helped me to record specific details of the interviews. Twycross and Shorten (2016) indicated that observation notes are useful for data

collection in qualitative studies. These may comprise additional information, such as body language, detailed conversations with participants, and researcher reflection of communication with the participant.

Englander (2019) noted that participants' responses guide the interview, but researchers used the interview guide to conduct qualitative semi structured interviews. I started by scheduling the interviews in advance at a convenient location and time for each participant. The open-ended questions were designed to capture data from participants by their descriptions and analyses. I then integrated the interactions into my observation notes and coded their views into common themes, similar to the approach described by Mann (2016).

After I coordinated the interviews, I organized the thematic analysis of the collected data and calculated each theme's frequency to determine specific factors as described by Tai and Ajjawi (2016). Observational notes, member checking, and interviews were used to achieve data triangulation. I also provided each participant with a summary of their interview following the member checking process. Member checking is used for exploring the credibility of results in qualitative research and allows participants to validate the data collected after the interview (Birt et al., 2016). Data collected were returned to participants to check for quality and accuracy. Participants reviewing the data collected during member checking would ensure approval and allow the researcher to capture participants' honest responses (Thomas, 2016).

Data Collection Technique

The data collection technique used for this study was the interviewing of owners of small businesses. The interview method was suitable for this research study because it offers the opportunity to uncover data that cannot be accessible using other techniques such as observations and questionnaires (Oltmann, 2016). Interviewing is not just a data collection tool, but rather an interactive means used to gain information; as such, it has its advantages and disadvantages. The advantage of using interviews includes controlling the answering order, relatively flexible interaction, and a high return rate with the presence of the interviewer (Hunter, 2017). The interview questions were simplified and rephrased to ensure a shared understanding between the interviewer and interviewees. As a result, more appropriate answers can subsequently produce accurate data (Hunter, 2017).

Furthermore, the interview method is inexpensive compared to other data collection techniques; these advantages have made interviewing an attractive method for my study data collection. However, like any other data collection technique, interviews have disadvantages; although interviewing is among the most used data collection technique, it can only be useful in small-scale study research and can be deceptively difficult because the perceptions can change over time pending on the circumstances and responses that might be considered biased and potentially inconsistent (Hunter, 2017). More so, the interview process is time-consuming with both data collection and analysis that need to be transcribed, coded, and translated. After IRB approval, I began to conduct face-to-face, semistructured interviews as stipulated in the interview protocol (see Appendix B). I used an audio recorder to capture conversations and record interviews,

which is an acceptable process for collecting data through an interview; this was a similar process used by Clark and Veale (2018). I conducted the interviews personally rather than through the phone, in which the interview process assisted me in analyzing participants' body language, which was a similar process used by Oltmann (2016).

In the first interview question, I considered strategies used by owners of small businesses to protect their business data against cyber attacks, and the interview question was further developed. The interviews were face-to-face, and I used open-end, semistructured questions, which permitted me to collect data while trying to understand the dynamics of the interview (Weis & Willems, 2017). I also observed the interview protocol and conducted a follow-up question for clarity, which is a similar process described by Clark and Veale (2018). I followed a detailed workflow to support consistency with all the interviews. This workflow includes a list of thorough questions for the participant, a summary statement, and a member-checking follow-up with a reminder to participants similar to the process used by Van de Wiel (2017). It is imperative in qualitative data interpretation for the researcher to guarantee reliability and validity. I used member checking for data interpretation by summarizing and restating the information and asked the participant to determine the similar validation process described by Birt et al. (2016). Some of the participants either disagreed or agreed that the summarized information reflected their experiences or views and when completeness and accuracy were assured, this step provided the necessary accuracy and credibility.

Data Organization Technique

I recorded the interviews using an audio recorder similar to the approach used by Castillo-Montoya (2016). I later transcribed all recordings into a Word document. Weis and Willems (2017) recommended a process for organizing and securing data. I organized and secured both the transcribed documents and audio recordings and backing them up to a private cloud account. During the interview process, I wrote down notes that detailed my observations. I used thematic analysis process to analyze the transcripts; this helped me to identify common themes and calculating the themes' frequencies, as described by Maguire and Delahunt (2017). I used Nvivo to note and calculate the thematic analysis and also backed up all documents in the private cloud account. All files were stored in the private cloud account for five years, after which, will be securely deleted from the private cloud account.

Data Analysis

I collected data through semistructured interviews. I supported participant responses by reviewing and analyzing business archival documents on IT security procedures that were obtained from participants. The process of data analysis involved investigating and transcribing digital audio recordings, semistructured interview transcripts, member checking notes, and reviewing other field notes and comments to help simplify the data analysis. Qualitative researchers typically employ software to collect, organize, and examine data from interviews, review documentation, and field notes (Yin, 2018).

Using software for data analysis is very helpful when conducting a semistructured qualitative study, and selecting the correct software will help to increase research accuracy. *NVivo* is a user-friendly product that provides qualitative data analysis and enables researchers to generate projects and manage data based on various study designs (Zamawe, 2015). *NVivo* supports data retrieving, sorting, categorizing, browsing, coding, interpreting, and synthesizing researcher qualitative data (Zamawe, 2015). I used the program because it offered features that allowed me to analyze and automate data that were generated from the selected inputs, as described by Paulus, Woods, Atkins, and Macklin (2017); Phillippi and Lauderdale (2017). I used Nvivo to analyzed the transcript based on the interview transcripts and further subcategorize the data based on their parameters. Nvivo was very helpful in organizing, analyzing, and classifying non-numerical data from a similar process described by Zamawe (2015). I analyzed and transcribed the interview transcripts and observational field notes from participants' responses, similar to the approach described by Boddy (2016). I used *NVivo* to code participants' responses into themes by using a thematic analysis technique, as described by Zamawe (2015). After entering the data into *NVivo*, I used the coded data to generate multiple data sets as it relates to how owners of small businesses are protecting confidential company data from cyber attacks. I was able to remove unrelated data and evaluate the remainder with an unbiased approach while maintaining the original data set. Analyzed results included descriptions, themes, and the factors that influence owners of small businesses' decisions as it relates to protecting confidential company data from cyber attacks.

After analyzing the data, I described the interpreted data and presented the findings in section 3 of the research study. Alongside thematic analysis, I also utilized observational notes to ensure that I captured all related and essential data. Alongside thematic analysis, I also utilized observational notes to ensure that I captured all related and essential data. The observational notes were used as a supplement to the interview responses and archival documents on IT security procedure response plans, as discussed by Phillippi and Lauderdale (2017). Member checking was a process used to increase validity, while data triangulation was used to ensure and test the validity of the findings as described by Tibben (2015). I correlated the key themes from the data to address the research question, I used the primary components emerging from interviews to connect current literature and conceptual frameworks as a means of evaluating, interpreting, and organizing the collected data.

The search terms from the literature review that was used to capture data are *cybersecurity strategy, system security strategy, outsourcing strategy, implementing security procedures, cybersecurity awareness education and training*, and I then analyzed the data using GST and RAA. Researchers use GST as a framework for understanding complex cybersecurity systems and implement strategies to change their focus from defensive to offensive approaches (Stitilis et al., 2016). Leukfeldt and Yar (2016) noted that the RAA would be a useful analytical framework to study cybercrimes, identify vulnerable targets, and serve as a means for adopting and enforcing cybersecurity policies.

Reliability and Validity

Reliability and validity are crucial in this study. To establish and obtain accurate data measurement, I concentrated on data triangulation and dependability, similar to the approach used by Motoyama and Mayer (2017). To establish and obtain validity, I used the concepts of conformability and transferability. Trustworthiness in qualitative research studies consists of dependability, credibility, transferability, and confirmability (Korstjens & Moser, 2017). I will further discuss how I obtained reliability and validity in the following section.

Reliability

Renz, Carrington, and Badger (2018) pointed out that reliability could be achieved through triangulation and dependability. I used dependability to seek reliability because it defines the degree to which the research findings produce consistent and stable results. Birt et al. (2016) concluded that participants' validation is an essential component in qualitative research that helps researchers to check for resonance and accuracy in participants' responses. To improve dependability, I used several data sources: (a) review and conduct semistructured interviews; (b) used interview protocol in Appendix B to administer all interviews; (c) applied member checking, and (d) used observational notes to examine the collected data for consistency. Interview questions were not focused on specific organizational initiatives, but rather the findings were based on participants' responses. I took accurate notes while actively observing responses to replicate the interviews that helped to established research study dependability, similar to the process used by Collingridge and Gantt (2019). To ensure the mutual reliability and legitimacy of

the findings, I established research quality. Amankwaa (2016) noted that research study trustworthiness is essential in creating the value of a study.

Validity

Validation and verification of data help to improve the validity and credibility of research findings. Participants could validate the data collected from the interview through member checking to determine the data credibility. I seek participants' perspectives, which helped to maintain validity and credibility. Participants were able to verify the interview data and provide their opinion; this helped to validate the collected data and improve its credibility. Qualitative research data verification and validation use corroboration from participants through member checking (Birt et al., 2016).

As I collect data, I considered all repetitive behaviors or actions as a way of maintaining the credibility process, as described by Nelson (2016). Davidson, Paulus, and Jackson (2016) noted that interviews are a standard method used to collect data in qualitative research. I collected data through face-to-face, semi structured interviews using an interview protocol. Renz et al. (2018) further described that transferability is synonymous with external validity or generalizability. Transferability could be recognized when readers are provided with evidence that the research findings could apply to other situations, contexts, and populations. To ensure applicability and transferability to other situations, I maintained a thorough note and documentation, along with geographic limitations, as it relates to the interviews in order to ensure that transferability applies to findings from similar projects. A transferability limitation in this study would be geographic because the research was conducted only in Fort Lauderdale,

Florida. Confirmability signifies the extent to which other researchers can confirm or corroborate the research study results. These helped determine the level of objectivity related to the study (Renz et al., 2018). I developed a review trail, and this was a unique way to adopt confirmability, which allowed me to remain in the background during the study (Connelly, 2016). I ensured validity by taking several precautions. First, as described, I never had initial contact with participants before IRB approval. Second, I listen to the viewpoints of participants without bias, which assists in preserving the integrity of the interview process. Third, I followed the data analysis procedure outlined in the previous section, which ensures that I maintained the standard used in prior studies to validity data (Connelly, 2016). Data saturation is significant because it indicates data accuracy, and this can occur when no further categories or themes are derived from the collected data (Benoot et al., 2016). In a multiple case study design, the pool size of four interviewees, and the qualitative interview technique are essential requirements for achieving data saturation (Boddy, 2016). Because the study did not reach data saturation after four interviews, I conducted more interviews after no new information was received, I attained data saturation, which was a similar approach described by Benoot et al. (2016). The research study consists of various methods for comparing, associating, and cross-checking data that helped to increase the study's reliability and validity.

Summary and Transition

In Section 2, I described the research purpose statement, the role of the researcher, and I addressed how participants were selected and detailed the research methodology and design. I further defined the sampling tactics and how I used these. I detailed the data

collection instruments, techniques, organization, and analysis. Section 2 ended with ensuring study reliability and validity. I begin Section 3 by presenting the overview findings, professional practice, the implications' social change, recommended action, further research recommendations, my reflection and experience during the process, and conclusion.

Section 3: Application to Professional Practice and Implications for Change

Introduction

The purpose of this qualitative multiple case study was to explore strategies used by owners of small businesses to protect confidential company data from cyber attacks. All participants that were interviewed concluded that proactive security strategies were essential in mitigating data breaches. Through the combination of the interview data, literature review, and conceptual framework, I discovered the strategies participants used to protect their business against cyberattacks, which include four themes: (a) security information management strategy, (b) organizational strategy, (c) consistent security policy, and (d) cybersecurity risk management strategy. Additionally, the study findings support Von Bertalanffy's (1972) GST and Cohen and Felson's (1979) RAA. In the following section of this study, I confirm the connection between the themes identified and derived from the collected data and the conceptual frameworks.

Presentation of the Findings

The findings address the overarching study question, "What strategies do owners of small businesses use to protect business data against cyber attacks?" I applied a practical working framework, such as grouping the codes into categories using the NVivo software tool to help me identify themes that emerged, such as security information management strategy, organizational strategy, consistent security policy, and cybersecurity risk management strategy. I also categorized the themes and created

descriptions to identify the themes and noted the frequency as they occurred from the data set.

In Section 1 of this study, I was unable to find specific and current information for the literature reviewed, that directly related to the research question; this created a gap for further study. These research findings were consistent with evidence from the related concept of Von Bertalanffy's (1972) GST and Cohen and Felson's (1979) RAA, which were both conceptual frameworks for this study. The GST theory is a process used to explore data that correspond with: (a) system units, (b) collaborative exchange and continual relationships within the system, and (c) analysis of systems. The GST theory provides a way of interpreting and viewing internally connected units, as suggested by Aydiner, Tatoglu, Bayraktar, and Zaim, (2019), of the cybersecurity strategies used by owners of small businesses. Owners of small businesses use internally connected units to reach various parts of their systems, such as information security (Chalvatzis et al., 2019). All participants agreed that protecting business data was a critical component to the success of their organization, and implementing cybersecurity is crucial to their growth. Managing information security strategy and organizational strategy were both predominant prevention coding nodes during the analysis of the interview data and archival documents.

The study findings support the concept of interconnectivity in GST, as demonstrated in the themes and subthemes; each theme was based on evolving and growing changes in cybersecurity. The GST was essential in understanding the interconnectivity of the system, which was a process used to explore strategies that

participants were using to protect confidential company data from cyber attacks. Instead of treating each theme and subtheme separately, owners of small businesses could consider collectively using the themes and subthemes to implement a holistic strategy to protect business data from cyber attacks.

The RAA was also useful in determining the potential motivation behind cybersecurity attacks and possible means for preventing and reducing cybercrime on small business systems, as proposed by Argun and Daglar (2016). The RAA outlined criminal behavior as motivated offenders with a proper target lacking capable guardians. Online-motivated offenders include hackers, fraudsters, stalkers, pirates, and other criminals (Reyns, 2015). An online target that is suitable for predation includes proprietary data, personal data, and online payment systems, along with vulnerable computer systems that may be disrupted and compromised by unauthorized interference and intrusion (Reyns, 2015). Capable guardians involve the various forms of cybersecurity, system protections, management access systems, ID authentication, firewalls, virtual private networks, and anti-intrusion. These are considered strategies employed by owners of small businesses to protect their business data against cyber attacks (Van de Weijer & Leukfeldt, 2017).

The consistent security policy and organizational strategy themes served as the coding nodes for creating a security plan, that demonstrated the presence of a capable guardian in place. The cybersecurity risk management strategy served as a prevention measure that reflects a coding node for a secured provider that also illustrated the presence of an intelligent guardian in place.

The four emergent themes regarding strategies used by owners of small businesses to protect business data against cyber attacks are (a) security information management strategy, (b) organizational strategy (c) consistent security policy, and (d) cybersecurity risk management strategy. A total of 254 collected references were counted from the coded contents. From the four emergent themes, managing information security strategy has approximately 79 references count with a total of 30.12%, the organizational strategy has approximately 66 references count with a total of 26.23% consistent security policy has approximately 56 references count with a total of 23.35%, and cybersecurity risk management strategy has approximately 53 references count with a total of 20.30%.

Theme 1: Security Information Management Strategy

Security information management strategy emerged as a major theme. Data were collected from five participant's responses and through reviewing IT security procedure documents from the five participants. The participants responded with the emerging subthemes for cloud storage implementation, access control, information strategy, security practice strategies, policy strategy. Information security refers to the protection of business and consumers' data from cyber attacks; this process could be used to protect data confidentiality, integrity, and availability by preventing unauthorized access, malicious intentions, disruption, modification and the destruction of data (Wang, Shan, Gupta, & Rao, 2019). Owners of small businesses could implement an information security strategy that can protect data confidentiality, integrity, and availability while maintaining effective productivity (Paliszkiewicz, 2019). The pseudonyms SB1, SB2, SB3, SB4, and SB5, are used to maintain participant confidentiality in this study. All five

participants stressed the importance of managing an information security strategy. SB1 stated:

> We integrated our strategy for protecting information into our core business process by publishing a well-defined security standard and information security policy. We also have a designated cybersecurity point person that is implementing all our IT solutions. Even without a dedicated IT staff, our designated cybersecurity point person is knowledgeable about cybersecurity. We have also established a security perimeter around our critical systems using multifactor authentication. To mitigate data risks, we adopted a single cloud security platform that controls users' device and network access, which is used to detect and mitigate threats in real-time. We managed access to data; our data are password-protected, and we demand an additional form of authentication. We configured the authentication to issue a one-time PIN before the individual can have access to the data.

In agreement with SB1, SB2 mentioned:

> We have established a successful way of managing our information security program; the program begins from upper-level management. The program consists of building data protection in layers; we setup appropriate access rules to information management, thereby reducing vulnerability. As part of managing our information security, we doubled our firewall to add redundancy. We also used email filtering in addition to continuous threat protection to scan inbound emails to avoid any potential threats from both links and email attachments to prevent

> malware attacks from entering our network system. We also compartmentalizing our network to enforce network separation and use commercial software to monitor network traffic and identify unauthorized attempts they may want to change, delete, or cause damage information. Also, we backed up all user workstations and company servers to a cloud server at a different geographical location. The average cost of cloud storage is less expensive but very helpful in protecting our business data against ransomware and phishing attacks.

SB3 noted:

> We practice protecting login credentials for network hosts, which is also crucial in defending business data against cyber intruders. We also implemented and installed some system security tools like firewalls, antivirus, encryption, a virtual private network (VPN), passwords, and biometrics software. We have also implemented a business continuity plan that frequently back-up our business data in the cloud. We also conduct regular information security testing on our systems. We currently use a third-party cybersecurity company for penetration testing to ensure compliance and protection procedures against any possible cyber breach.

SB4 acknowledged that "our strategy involves basic system security practices, which require the implementation of strong passwords, secured web applications with firewalls, and we also use an automated malware scanner to scan our system regularly. We easily sync files and folders from our computers and mobile devices to our backup cloud system." SB5 indicated that "my organizational data are automatically backed up to the

cloud regularly. Our operating system's firewall is enabled and set to prevent outsiders from accessing data on our network."

Managing information security is to minimize risk and guarantee business continuity by actively limiting cybersecurity risk (Tu, Yuan, Archer, & Connelly, 2018). Owners of small businesses must improve their information security strategy to ensure capabilities provided aligns with their business goals by implementing an effective way to identify and address potential threats and vulnerabilities (You, Oh, Kim, & Lee, 2018). Sensitive data should be adequately secured; no individual should have access to information beyond their access privilege. Owners of small businesses could avoid granting classified access, as superiority within the organization, does not permit greater access. Likewise, compartmentalization access controls on a network to limit communication between systems can be used to identify unexpected and unauthorized attempts on the network (Sabitha & Rajasree, 2017). Lateral compartmentalization protects systems from unintentional interference by unqualified or unauthorized persons, which is a process used to reduce potential threats and vulnerabilities.

Owners of small businesses could enforce access control policies based on compartmentalizing how sensitive data can be accessed (Sabitha & Rajasree, 2017). Compartmentalization of business data is a process used to mitigate an insider and external risks, by segmenting access to a network, the goal is to reduce the scope of data compromise. Cloud storage implementation emerged as a sub-theme; the coded contents have approximately 47 references count with a total of 49 %.

Cloud storage implementation. The subtheme from the security information management strategy was cloud storage implementation. The cloud storage implementation subtheme emerged from five participants' responses and through reviewing IT security procedure documents from the five participants. Cloud storage is a computing model that allows businesses to store data in the cloud using the Internet (Yuhuan, 2017). Cloud storage vendors maintain the capacity, security, and durability that makes cloud storage data accessible and secured, thereby allowing owners of small businesses a means of protecting their business data against cyber attacks. Kalaiprasath, Elankavi, and Udayakumar (2017) noted that cloud storage implementation is adhering to privacy and security policies that guarantee users' data are fully secured. Participants had different responses concerning appropriate data protection with cloud vendors. Senarathna, Yeoh, Warren, and Salzman (2016) discovered that security and privacy features have less influence on why owners of small businesses are adopting cloud computing. Participants who rely on cloud storage for their business benefit from the security services; they are also using the services for allocation, distribution of access control, monitoring, and protecting their business data against cyber attacks. They back up their files in cloud storage, which is an essential source for business continuity in the event of a system crash, cyber breached, or data loss. Owners of small businesses can implement cloud computing at a reasonable price that can guarantee access to data and applications from anywhere. Implementing cloud computing also gives businesses access to previously out of reach technologies, which is helping them develop and improve operational processes (Henry & Ali, 2017).

Cloud storage can also assist in verifying and protecting business and consumers' data at rest, in motion, or use in the cloud or on business premises with services that include unified sharing of computing resources. One of the most comfortable and most efficient ways for owners of small businesses to tackle cybersecurity needs is to backup critical business data and applications in the cloud. The organization can securely synchronize business data from the cloud to workstations and other work-related devices without losing any data or data ever leaving the server. The organization can also store data in a secure location that can also capture cloud backup.

Kalaiprasath et al. (2017) concluded that security controls and compliance models could be used to manage the risk associated with potential cloud storage threats. The study developed a semantically rich ontology that could be used to model threats, controls, and cloud security policies. Owners of small businesses could formulate their cloud storage security policies to include security controls and compliance models to protect business data in the cloud.

Theme 2: Organizational Strategy

The second major theme is the concept of organizational strategy, which emerged after analyzing participant responses and reviewing IT security procedure documents from the five participants. James (2018) researched supported this study by affirming that an organization's security strategy must align with its business strategy and should be an integral component of the top management decision-making process. I reviewed participant interviews and archival documents. All five participants stressed the importance of implementing an effective organizational strategy. Carias, Labaka,

Sarriegi, and Hernantes (2019) acknowledged organizational strategy as cybersecurity preparedness that integrates employee training and technical security to measure and manage cyber attacks while effectively continuing its business operation. Boiko, Shendryk, and Boiko (2019) described an effective organizational cybersecurity strategy as a technique used by business leaders to align risk associated with cybersecurity and their critical operations. The study findings below described the emerging subthemes which are (a) awareness education has approximately 40 references count with a total of 35.54%, (b) employee training has approximately 39 references count with a total of 33.27%, and (c) people's management has approximately 37 references count with a total of 31.19%.

Awareness education. The first subtheme to emerge from analyzing data from the organizational strategy was awareness education. Awareness education is one of the resources that businesses depend on to prevent and protect confidential company data from cyber attacks (Irons, 2019). Owners of small businesses should be aware of the constant increase in data breaches, phishing, and ransomware attacks. Awareness education involves knowing how to protect organizational data and how to take practical steps to prevent data breaches.

SB1 stated, "our team performs awareness education to keep our organization updated with the latest threats and making sure that our systems are safe from hackers or any form of breach attempts. By instituting awareness education, owners of small businesses could understand the current security vulnerabilities and heighten the chances of catching an attack before it is fully enacted, thereby minimizing the damage and

reducing the cost of data breach recovery (Bhardwaj & Goundar, 2019).” SB2 replied that “we conduct repetitive training and ongoing awareness; sometimes we even conduct random testing to analyze security vulnerabilities within our system and areas of exploitation and educate our employees on how to prevent vulnerabilities. The most prevalent IT security threat that owners of small businesses are facing is the fact that they lack the awareness of security vulnerabilities (Bhardwaj & Goundar, 2019). Owners of small businesses could promote cybersecurity awareness education to prevent and overcome potential threats.” SB3 stipulated that “we created and instilled security awareness culture within our organization in a modified manner, by working with the IT manager to interpret security verbiage into simple procedures that every employee could easily understand and follow. Based on these guidelines, we provide constant training to all employees on how to access and safeguard critical business systems, and we guarantee that they understand and apply this concept to help us mitigate possible risk exposure to our system.”

SB4 also stipulated that “we have developed a risk management strategy that consists of situational awareness and an acute awareness of customers' personal information, limits access, and monitors network system.” SB5 replied that “we hired a security company to educate our staff on the current threats; they also evaluate our system and perform cybersecurity awareness. Every three months, we perform risk assessment, which is helping us to identify risks and vulnerabilities in our network. Our security awareness program is a process used to rate severe vulnerabilities, determine the effectiveness of our current security resources, and the cause of action.”

The data revealed that participants recognized and implemented awareness education and provided employees with the essential understanding of imminent and ongoing cyber threats, and also prepare them to be the first line of defense and be vigilant against frequent cyber attacks and threats. All employees with access to a work-related mobile device and computer undergo a thorough awareness education, which includes maintaining physical security, password management, online security, and how to detect system vulnerabilities, phishing, and malware defense simulations (George & Thampi, 2019). By implementing cybersecurity awareness and training, owners of small businesses could heighten the chances of mitigating an attack before it is fully enacted, minimize the damage to the business brand, and reduce recovery costs (Irons, 2019).

Awareness education should be implemented on three levels: creating, delivering, and evaluating the program. Over time, the program can have steadfast quarterly and annual goals that would become increasingly directed towards the occurrence and severity of actual incidents that arise within the organization. Cybercriminals are continually seeking new and sophisticated ways of exploiting security weaknesses; security awareness education is a means in which organizations are equipping their employees to react to the latest successful exploit of the organization. Effective cybersecurity awareness education should integrate organizational, legal, and best practices of security technologies, this can progress the information assurance of small businesses (Dai, 2018). An essential and affordable action is for owners of small businesses to continually conduct a security assessment to identify vulnerabilities. Once vulnerabilities are recognized, owners of small businesses can create a response plan on

how to mitigate threats and losses in the event of an attack.

Awareness training activities should include details of employee preparedness in the event of a breach. The security awareness should provide every employee with the fundamental understanding that there are imminent and ongoing cyber threats, preparing employees through constant cybersecurity training for common cyber attacks and threats. Due to the rapidly changing technological environment and the extensive vulnerabilities, the effectiveness of the awareness education cannot be measured based on past security assessments. Instead, to ensure its success, awareness education must be tested continuously and update regularly. Cybersecurity awareness education must be efficient, repetitive, and continuously tested to safeguard and protect organizational data (Irons, 2019).

Employee training. The second subtheme to emerge from analyzing data from the organizational strategy was employee training. Training involves teaching employees the strategies that would help guarantee preparedness and optimized defensive responses to cybersecurity threats. Howell (2016) pointed out that employee training could best be implemented in the simplest terms of providing employees with the necessary knowledge and skills that can prepare them on how they can protect the business system from all forms of attacks. Participants' responses and review of their security procedures revealed that all participants had some form of employee training. SB1 stated that "we conduct cross-section training for all store managers. While the manager is in charge of training employees based on safeguarding operating systems, reporting system outages, and reduced email scams and identified social phishing." SB2 also indicated that "we

provided and scheduled multiple cybersecurity training sessions for our employees based on their availability, but for new features in our software, our reliability is on our vendors to provide those training." SB3 stated that "we provide constant training to all employees on understanding and accessing systems and to ensure they comprehend the proper use of the business system(s), which has ultimately helped in lowering our potential risk exposure to security issues." SB4 emphasized that "managers understand their security requirements and are responsible for conducting quarterly employee training, and employees understanding how to spot suspicious attempts by becoming the first line of defense, thereby assuming the role of protecting business and customer data."

SB5 also indicated that "as part of our business policies, we are educating and training every new employee on security measures. We also are conducting quarterly training for all our employees on the latest security measures, and how they can help keep our system safe." The findings showed that each participant implemented education awareness and training as a way of defending against cyber attacks. Data security is paramount to organizational success; as such, it is paramount for small businesses to develop employee training that would address how data can be handled and how to identify and mitigate threats to data security. Proper employee training should include these elements: current threat assessment, red flag attack, preventive procedures, and mitigating plans. Network security and awareness education training should be based on cyber attack simulations that are consistent with current trends. Cyber attacks evolve in their technologies and approach; as such, owners of small businesses must upgrade defensive training to keep system vulnerabilities low (Meyers, Hansen, Giboney, &

Rowe, 2018).

Owners of small businesses could also create cybersecurity awareness and employee training protocols as a countermeasure against attacks and protect the confidentiality of business and customer data (Rocha Flores & Ekstedt, 2016). Employees are becoming the most critical aspect of cybersecurity preparation were eliminating human error seems impossible. However, owners of small businesses can minimize cybersecurity risk by continuously and consistently testing and educating employees to become defenders against cybersecurity threats by developing their knowledge of cybersecurity, thereby improving employee behaviors toward cybersecurity preparation. Employee cybersecurity training should include ways of identifying all kinds of threats, how to respond to phishing emails, how to avoid visiting malware-infected web pages, and also how to implement a two-step verification and access confidential information (Howell, 2016).

Peoples management. The third subtheme to emerge from analyzing data from the organizational strategy was people's management. Owners of small businesses could no longer overlook the concept of managing people's cybersecurity behavior. They would have to implement cybersecurity policies that would manage and guide employees' cybersecurity behavior. Although technology solutions play a vital role in protecting business assets, users are often the weakest link in information security. A new challenge for owners of small businesses is the ability to manage and guide employees' information security behaviors. Budzak (2016) concluded that users' behavior is becoming a threat to information security. Gangwar and Date (2016) noted that people are the primary source

of information security incidents. People's management subtheme emerged after reviewing the participants' responses and through reviewing IT security procedure documents, in which all participants agreed that managing and guiding employees' cybersecurity behavior is vital to protecting information security. Udroiu (2018) noted that without employees who are dedicated and steadfast in doing their part to ensure that significant business systems and information assets are safe, good security practices would be impossible to carry out. Owners of small businesses could develop strategies on how to manage and guide employees' information security behaviors, by evaluating the effectiveness of their information security behavior, and determine ways to improve employees' behavior. Owners of small businesses should focus on improving information security strategies to find ways to manage and motivate employees to protect organizational information assets. Owners of small businesses should not minimize the significance of human factors in information security because users could intentionally or negligently pose a substantial threat to organizational information security (Sollars, 2016). Owners of small businesses should recruit and motivate staff to follow their security policy guidelines and encourage them to be vigilant in protecting organization information security (Sollars, 2016).

Theme 3: Consistent Security Policy

The third major theme that emerged in this study was a consistent security policy. The theme emerged from five participant's responses and through reviewing IT security procedure documents from the five participants. Information security policy is defined by San Nicolas-Rocca and Burkhard (2019) as a document that identifies rules and

procedures that guides how the organization's IT resources and assets are accessed. Schulz (2019) noted that effective and consistent IT security policy is a model of the organizational culture in which procedures and rules are driven from its employees' approach to organizational information security. Almeida et al. (2018) further described that information security policy must reflect the support and commitment that owners of small businesses have for information security and demonstrate the role it plays in the overall organizational strategy. A small business information security policy should offer guidelines to employees on how to handle everyday information security tasks. The participant interviews and through reviewing IT security procedure documents from SB1, SB2, SB3, SB4, and SB5 showed that all participants are maintaining IT security policy. The reviewed documents provided details on how these owners of small businesses are defending their business data from a cyber breach. Based on this analysis, participants are continuously improving their IT security policy to protect business data against cyber attacks. SB1 indicated that “we implemented security policies and procedures that we directed towards enhancing our internal network security tools. Our current policies and procedures are efficiently guiding the flow of data and protect our businesses from cyberattacks.” One of the issues facing owners of small businesses is the nonexistence of consistent IT security policies, which is a process used to respond to cyber attacks and also protect against unforeseen threats. SB1 also noted that “we configured our systems to track data distribution as part of our data protection regulations.” SB2 stated that “we regularly update our IT security policy to preserve the confidentiality, integrity, and availability of our information systems and how members of our organizations access

information." After reviewing the IT security policy document from SB2, the policy describes how the responsibilities and functions of each individual in the organization as it relates to protecting business data from a cyber breach. The IT security policy also categorizes how authority is granting security personnel and identify and detail data is transmitted in their network. The IT security policy of an organization is a set of rules that prescribed the organizational network structure and also ensured how users could access data within the boundaries of the organization network.

SB3 stated that "we also practice internal system control, such as creating unique login information, a valid password to access business systems, and we instituted a policy that requires a password change between 45 and 90 days contingent on the sensitivity of the access data." SB4 stated that "we also have a cybersecurity policy that governs Internet usage and the penalties for violating the policy. Our policy also describes how we handle and protect business and customer data." SB5 stated that "we have a policy in place that ensures all employees that work from home are firewall-protected and encourage the use of VPN to connect to our central system." Owners of small businesses must continue to invest in a proactive approach to protect confidential data. I reviewed participants' IT security policy documents to ensure that a consistent security policy is in place. I included some extracts from SB4's IT security policy documents as a means of triangulating and validating the data collected from the interview: The security policy objective is to protect our business and customer data from illegal access. The security policy entails how data and applications are accessible and used for essential and continued operations of the business. There shall be no alteration or deletion as a result of

intentional or accidental attempts to gain or compromise access to business computer systems. The security policy is related to all users who have access to our system and network administrator that is responsible for operating workstations and data backup. The business process must adhere to the organization's security measures, as it is essential to our business continuity. This security policy articulates the complexity of information security. If there is a need for change at any level of this policy, the changes must be evaluated by our legal counsel. Mermigas and Pirounias (2018) noted that organizations should accept that security policy is an essential cost, and the best way to improve and manage the cost associated with security policy is by developing procedures around a robust security framework. The continuous increase in cybersecurity attacks has led to businesses investing and maintaining a consistent security policy. A consistent security policy is a process that uses no-compromise protection against cybersecurity attacks, with consistent implementation of policy at every level. All-inclusive protection is directed to stop cybersecurity attacks. A security policy offers guidelines that make it different from security procedures and processes. Security policy provides both specific and high-level guidelines on how the organization is protecting its data but will not stipulate the precise implementation. These provide the scope to choose which type of security methods and devices that would best fit the organizational budget. A consistent security policy must maintain a standard, enforced, and communicated throughout the organization. Owners of small businesses can now create a consistency security policy across what were substantially different security policies and implementations. This consistency method will help owners of small businesses avoid conflicts in policy that add misperception, run

up costs, and increase vulnerabilities.

Theme 4: Cybersecurity Risk Management Strategy

Cybersecurity risk management strategy was the fourth main theme in this research. The theme developed from five participants' responses and through reviewing IT security procedure documents. The emerging subthemes are adopting a 3rd-party vendor, consulting IT experts, and limited liabilities. The findings correlate with that of Kure, Islam, and Razzaque (2018), who described cybersecurity risk management as a fundamental and essential process for managing risks associated with data breaches. Owners of small businesses would be able to identify, evaluate, and mitigate the risk associated with the availability, confidentiality, integrity of their business, and customers' data. Governments are implementing regulation that may impact businesses that do not have the proper process of handling business and customers' data. For example, the general data protection regulation (GDPR) is an EU regulation that governs the processing of personal data. The policy requires that all businesses protect data from attacks, but primarily to protect consumer data from transactions that arise within and outside EU member states (Denley, Foulsham, & Hitchen, 2019). GDPR applies to all business selling to and storing personal data of EU citizens, including the business organization from other countries. The GDPR affects all types of companies that collect and process personal data (Munier & Kemball-Cook, 2019). Examples of data include names, telephone numbers, customer data, e-mail addresses, or any form of identifiable data (Denley et al., 2019). The GDPR policy applies to all businesses irrespective of where the business process took place; as such, failure to comply with this policy would

incur penalties. Owners of small businesses would need to implement a cybersecurity risk management strategy with security procedures and invest in security technology and IT experts to protect their business data against cyber attacks. Also, it is vital to note that protecting organization data would require implementing robust and comprehensive business solutions. Owners of small businesses can hire IT expert consultants as a cost-effective way to bridge the gap in skill, knowledge, and IT solutions is a process used to avoid vulnerabilities, minimize and mitigate cybersecurity risk (Drechsler, & Weibschadel, 2018). Owners of small businesses can also invest in a third-party vendor that can provide cybersecurity preventive procedures and business services that would allow them to remain compliant with PCI DSS regulations. The study findings below described the emerging subthemes which are (a) adopting a 3rd part vendor has approximately 47 references count with a total of 34.44%, (b) consulting IT experts have approximately 45 references count with a total of 33.27%, and (c) limited liabilities has approximately 42 references count with a total of 32.29%.

Adopting 3rd party vendor IT. The concept of adopting 3rd party vendor IT was the first subtheme created from cybersecurity risk management strategy. All participants stated that they depend on 3rd party vendor IT services to avoid the risk associated with payment processing to protect their business data against cyber attacks. Reviewing the participants' security and procedure documents showed that they observed: "Payment Industry Data Security Standards (PCI-DSS), is a process used to safeguard and regulate data for cardholder payment." SB1 emphasized that "I rely on a third-party vendor for payment processing to avoid risk." SB2 said that "I depend entirely

on a third-party vendor for payment services; they absorb all burden and risks while limiting our liability against losses should there be any." Also, SB3 indicated that "our third-party vendor handles all our payments, thereby limiting our liability by protecting our business and customer data against a cyber breach." SB4 stated that "part of our strategy was to invest in a third-party vendor that is using SSL technology to optimize security for debit and credit transactions, thereby protecting cardholders against the misuse of data." Participant SB5 established a similar reliance on a third-party payment system: As stated, "We invested in a third-party payment system because it is safe and allows us to comply with financial regulation. It is difficult for our company to observe all the financial regulations; as such, we expand the scope of our third-party agreement to include how they handle our customers' data." New regulation compliance adds responsibilities and costs to owners of small businesses; the benefit of outsourcing payment systems compensates the liability and risks of having an internal payment system. Cybersecurity risk management strategy is to provide information and tools necessary to tackle data theft. Data theft has become a significant threat facing owners of small businesses. Owners of small businesses could use these tools to make better business decisions to help reduce data risk and protect business data against cyber attacks. Owners of small businesses also must understand the regulatory risks and identify steps that they can use to mitigate the risk. Owners of small businesses must adopt and integrate a cybersecurity risk management framework to assess and manage consumers' data in a proactive manner. Cyber risk management services do not only reduce the risk associated with cyber attacks but actively include compliance with

payment system regulation (Talesh, 2018). The strategy can also identify and quantify data risk and provide a cost-benefit analysis of potential mitigation. The cybersecurity risk management strategy would provide a risk-weighted analysis that owners of small businesses can use to base risk retention, reduction, sharing, transferring, and decision avoidance.

Consulting IT experts. The concept of consulting IT experts emerged from four participant's responses and after reviewing their security and procedure documents**.** Owners of small businesses can consult with IT experts to identify areas where their business system is vulnerable to cyber attacks and obtain recommendations that can be useful to protect business data against cyber attacks. Consulting IT experts' services include having a full assessment, implementation, and maintenance of the security systems. SB1 stated that "we consulted with IT experts, before creating our comprehensive incident response plan and monitoring tool that we are using to ping an IP address that tries to breach our security." An IT expert who specializes in anticipating and mitigating threats can provide an extra layer of protection that can prevent and minimize risks and quickly resolve any form of security issues. SB2 stated that "we use cybersecurity IT experts to develop and install patches in our network to protect our system from an attack." SB3 also indicated that "every year, we consult with an IT expert to conduct system penetration and testing to evaluate our system weakness and provide security controls that are adequately mitigating any perceived data risk." SB4 emphasized that "we consult with IT experts to conduct system checks to identify vulnerabilities, assess its immunity to attacks and provide recommendations to secure our system; we

were able to prevent further vulnerabilities in our systems." After reviewing SB1's IT security award, which indicates that they received commendations for relying on IT experts to provide secured services, these commendations were in their business bulletin. Cybersecurity IT experts are likely to have encountered virtually all forms of cyber attack and have found ways of dealing with the issues. As they are very familiar with the techniques that hackers are employing, they move faster when dealing with security issues. Cybersecurity has become a significant priority for small businesses looking to protect their business against the massive cost of data breaches. Cybersecurity IT experts are likely to find solutions quicker before any damage can occur since cybersecurity has become a significant priority for small businesses that are looking to protect their business against the massive cost of data breaches (Heller, Toregas, & Hoffman, 2019).

Limited liabilities. The third subtheme that emerged from analyzing data from participants demonstrates the implemented measure used to protect business and customers' data against cyber attacks. Participants responded by indicating their responsibilities and liabilities in the occurrence of a data breach; each participant agreed that adopting a 3rd party vendor helped limit their liability in the event of a data breach. SB1 replied that "the contract we have with our third-party vendor includes a limited liability provision." Owners of small businesses who utilized third-party vendors to secure business and customers' data tend to limit their cybersecurity liabilities, to prevent any form of losses in the event of a cyber breach. SB4 stated, "our vendor provides and maintains the confidentiality of our business and customers' data and are liable for any data loss." All participants indicated that their third-party vendor agreement also

stipulated that they have unlimited liability on their payment services. Participants' contract documentation with third-party payment providers indicates that if the business reports an account data or data breach. The business must retain a forensic investigator (PFI) to investigate the business processing system that the breached occurred; and if the evidence proves that the breach indeed occurred (Brown, 2016). The PFIs will give a detailed report to the card associations, on all the card data that is at risk and whether the business complied with PCI guidelines during the breach period. Owners of small businesses would then be required to provide all processed card numbers throughout the risk period. If the small business owner were not compliant during the risk period that led to the breach, they would incur the fine of noncompliance.

Applications to Professional Practice

Strategies used for protecting business data vary from small businesses to larger firms. The appropriate strategy may differ due to organizational size, but the factor remains that protecting business data is crucial to the survival of the business.

Ronchi (2019) concluded that technical countermeasures alone are not enough to protect against cyber attack; there is a need to uphold cyber defensive and preventive methods that can foster cybersecurity culture. The findings of this study might contribute significant strategies that could be useful to formulate cybersecurity strategies that owners of small businesses can use to protect their business data against cyber attacks. The findings might be significant to positive professional implications for implementing successful IT security systems in small businesses. Owners of small businesses might apply a cybersecurity strategy towards guiding their efforts and expenditures toward

structuring more secured business processes (Terlizzi, Meirelles, & Viegas Cortez da Cunha, 2017). Owners of small businesses could apply the identified themes in this study, which are (a) security information management strategy, (b) organizational strategy, (c) consistent security policy, and (d) cybersecurity risk management strategy. After an extensive review of current research, Campbell (2019) offered the opinion that for businesses to practice good cybersecurity, it would have to focus on counter actions that would include awareness, policies, processes, and continuous employee training towards cybersecurity compliance. These study findings include awareness, employee training, and people's management, which tends to increase owners of small businesses' resilience to cyber threats; and also provide their employees with the fundamental understanding toward cybersecurity compliance. All the described strategies, if implemented, can benefit owners of small businesses who want to protect their business data against cyber attacks. The findings of this study may also be used to create employees' knowledge base that can include cyber defensive and preventive methods used to reinforce employee cybersecurity awareness, to provide relevant training and consistent policy across all processes. The findings of this study align with evidence from the reviewed literature and might be relevant to extend knowledge gained from previous studies. The findings could provide owners of small businesses with appropriate strategies to further minimize cybersecurity risk. The application to professional practice consists of communicating the successful strategies that owners of small businesses are using to protect business data from cyber attacks. The results of my research showed that the application of active cybersecurity strategies, such as (a) security information management strategy, (b)

organizational strategy, (c) consistent security policy, and (d) cybersecurity risk management strategy, might be able to provide a foundational guide to other owners of small businesses who would like to develop and apply practical strategies to identify vulnerable targets and mitigate threats to protect confidential business data.

Implications for Social Change

The results of this study have the potential to generate positive social change that would increase customers' confidence, businesses' economic growth, and stimulate the socioeconomic lifecycle, resulting in potential employment gains for residents within the communities. Positive social change can be obtained through the implementation of this study findings to create a robust threat and vulnerability management program that can reduce consumers' exposure to security breaches and improve community engagement. Owners of small businesses could integrate a holistic cybersecurity approach that would enhance their cybersecurity to address all facets of incident preparedness, customer data security, legal counsel, and regulation that is tailored towards their business.

Findings from this study could provide owners of small businesses with four effective strategies that successful owners of small businesses have used to protect their business data against cyber attacks, which are (a) security information management strategy, (b) organizational strategy, (c) consistent security policy, and (d) cybersecurity risk management strategy. Owners of small businesses could implement and improve their cybersecurity strategies to eliminate future threats to their business and customers' data. The implications for positive social change might include applying and

implementing this study to increase consumer confidence and ensure better economic prosperity.

Recommendations for Action

The findings of this study are examples of strategies that some owners of small businesses used to protect confidential company data from cyber attacks. The recommended strategies are courses of action for owners of small businesses in the industry. The first recommendation is that owners of small businesses should develop an organizational strategy that will fully engage in active cybersecurity practices. Such a strategy should consist of policies and procedures that can be used to protect both business and customer data against cyber attacks. The second recommendation is that owners of small businesses could progressively link their business processes with cybersecurity policy to create a consistent security policy across their organization. The third recommendation is that owners of small businesses could also implement an effective strategy that they can use to address preparedness, data privacy, and response to data breaches in the event of a breach, which can have a positive impact on mitigating the effects of data breaches and protect confidential company data.

The findings and recommendations will be shared directly with the study participants. I intend to submit this study for publication and also seek opportunities to present the results at business workshops and conferences.

Recommendations for Further Research

The study findings might result in bridging the knowledge gaps on how owners of small businesses can protect their business and customer data from cyber attacks. Current

and future owners of small businesses might use the results of this study to cultivate consistent cyber security policy. Since this study was limited to Florida, there is a need for more research to be conducted, which should include other geographic locations. The findings may be different or similar based on the sample size and geographic data. Replicating this research study at a later time may yield different results as cybersecurity strategies may change over time.

A limitation that I mentioned in Section 1 was how participants could unintentionally provide insufficient data due to their limited knowledge of cyber security. However, participants supported their experiences with archived documents, which yielded the results of this research study. Participants were candid in their responses during the interviews, and they provided sufficient data for this study. My recommendation would be that future study researchers increase the sample size and geographic locations and compare the results to see if they are different or similar based on the increased sample size and geographic locations.

Reflections

I came to understand the types of successful strategies that owners of small businesses have used to protect both their business and customer data from cyber attacks, through the reviewed literature studies, completion of interviews and reviewing of archival security procedures documents. The DBA journey challenged me personally, academically, and increased my knowledge far beyond what I anticipated. Through the literature review and the interview process, my perspective was developed significantly on strategies that owners of small businesses can use to protect their businesses from

cyber attack. My perspective on the topic was developed because I had no preconceived notions about the research topic; I remained optimistic and kept a neutral view all through the research process. I relied on pre-existing research on the subject, and the data collected from interviewing participants and supporting documents. It was interesting to learn about new themes in cybersecurity strategies; my defined notion changed after completing the research study on cybersecurity strategies. This exercise has helped me to broaden my understanding, validate the purpose, and reason for researching strategies for implementing successful IT security systems in small businesses.

Conclusion

Past data protection studies have focused only on the technical aspect of a data breach incident, which is useful in helping organizations understand how a security breach occurred. The holistic cybersecurity approach that was included in this study finding incorporates process control, technical, and human aspects, which are the essential components for protecting data. Owners of small businesses can begin by taking the responsibility of protecting company data from cyber attacks by applying a holistic cybersecurity approach. My findings supported this approach by including (a) security information management strategy, (b) organizational strategy, (c) consistent security policy, and (d) cybersecurity risk management strategy to protect confidential company data from cyber attacks. Owners of small businesses could use these findings to formulate a cybersecurity strategy that could help to predict and eliminate future threats to customers' information.

References

Albahar, M. (2017). Cyber attacks and terrorism: A twenty-first-century conundrum. *Science and Engineering Ethics*, 1–14. doi:10.1007/s11948-016-9864-0

Ali, A. (2017). Ransomware: A research and a personal case study of dealing with this nasty malware. *Proceedings of the 2017 InSITE Conference*, *14*, 87–99. doi:10.28945/3661

Allodi, L., & Massacci, F. (2017). Security events and vulnerability data for cybersecurity risk estimation. *Risk Analysis*, *37*, 1606–1627. doi:10.1111/risa.12864

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

Alneyadi, S., Sithirasenan, E., & Muthukkumarasamy, V. (2016). A survey on data leakage prevention systems. *Journal of Network and Computer Applications*, *62*, 137–152. doi:10.1016/j.jnca.2016.01.008

Alves, T., & Morris, T. (2018). Hardware-based cyber threats. *Proceedings of the 4th International Conference on Information Systems Security and Privacy*, 259–266. doi:10.5220/0006577202590266

Amankwaa, L. (2016). Creating protocols for trustworthiness in qualitative research. *Journal of Cultural Diversity*, *23*, 121–127. Retrieved from https://www.ncbi.nlm.nih.gov/pubmed/29694754

Anders, G., Schiendorfer, A., Siefert, F., Steghofer, J., & Reif, W. (2015). Cooperative resource allocation in open systems of systems. *ACM Transactions on Autonomous and Adaptive Systems*, *10*(2), 1–44. doi:10.1145/2700323

Anderson, C., Baskerville, R. L., & Kaul, M. (2017). Information security control theory: Achieving a sustainable reconciliation between sharing and protecting the privacy of information. *Journal of Management Information Systems*, *34*, 1082–1112. doi:10.1080/07421222.2017.1394063

Angst, C. M., Block, E. S., D'Arcy, J., & Kelley, K. (2017). When do it security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches. *MIS Quarterly*, *41*, 893–916. doi:10.25300/misq/2017/41.3.10

Anton, N., & Nedelcu, A. (2015). The systemic approach to information protection in relation to risk in an integrated information security system. *Applied Mechanics and Materials*, *760*, 689–694. doi:10.4028/www.scientific.net/amm.760.689

Argun, U., & Daglar, M. (2016). Examination of routine activities theory by the property crime. *International Journal of Human Sciences*, *13*, 1188–1198. doi:10.14687/ijhs.v13i1.3665

Astani, M., & Ready, K. J. (2016). Trends and preventive strategies for mitigating cybersecurity breaches in organizations. *Issues in Information Systems*, *17*, 208–214. Retrieved from http://www.iacis.org/iis/2016/2_iis_2016_208-214

Awrey, D., & Van Zwieten, K. (2018). The shadow payment system. *Journal of Corporation Law*, *43*, 775–816. Retrieved from https://ora.ox.ac.uk/objects/uuid:2b881a4d-e34e-483d-b487-10c8f4a65429

Aydiner, A. S., Tatoglu, E., Bayraktar, E., & Zaim, S. (2019). Information system capabilities and firm performance: Opening the black box through decision-making performance and business-process performance. *International Journal of Information Management*, *47*, 168–182. doi:10.1016/j.ijinfomgt.2018.12.015

Bagschik, G., Stolte, T., & Maurer, M. (2017). Safety analysis based on systems theory applied to an unmanned protective vehicle. *Procedia Engineering*, *179*, 61–71. doi:10.1016/j.proeng.2017.03.096

Bai, G., Jiang, J., & Flasher, R. (2017). Hospital risk of data breaches. *JAMA Internal Medicine*, *177*, 878–880. doi:10.1001/jamainternmed.2017.0336

Balan, S., Otto, J., Minasian, E., & Aryal, A. (2017). Data analysis of cybercrimes in businesses. *Information Technology and Management Science*, *20*(1), 64–68. doi:10.1515/itms-2017-0011

Ban, H. J., Choi, J., & Kang, N. (2016). Fine-grained support of security services for resource-constrained internet of things. *International Journal of Distributed Sensor Networks*, *12*, 78–86. doi:10.1155/2016/7824686

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

Bennis, W. G., Katz, D., & Kahn, R. L. (1966). The social psychology of organizations. *American Sociological Review*, *31*, 745. doi:10.2307/2091895

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

Besliu, D. (2017). Cyber terrorism – A growing threat in the field of cybersecurity. *International Journal of Information Security and Cybercrime*, *6*, 35–39. doi:10.19107/ijisc.2017.02.05

Bhardwaj, A., & Goundar, S. (2019). A framework for effective threat hunting. *Network Security, 2019*, 15–19. doi:10.1016/s1353-4858(19)30074-1

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

Bohm, D., & Kuhn, T. S. (1964). The structure of scientific revolutions. *The Philosophical Quarterly*, *14*, 377–379. doi:10.2307/2217783

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

Brewer, R. (2016). Ransomware attacks: Detection, prevention, and cure. *Network Security*, *9*(1), 5–9. doi:10.1016/s1353-4858(16)30086-1

Brown, H. S. (2016). After the data breach: Managing the crisis and mitigating the impact. *Journal of Business Continuity & Emergency Planning*, *9*, 317–328. Retrieved from https://www.ncbi.nlm.nih.gov/pubmed/27318286

Bruce, A., Beuthin, R., Sheilds, L., Molzahn, A., & Schick-Makaroff, K. (2016). Narrative research evolving: Evolving through narrative research. *International Journal of Qualitative Methods*, *15*(1), 1–6. doi:10.1177/1609406916659292

Budzak, D. (2016). Information security – The people issue. *Business Information Review, 33*, 85–89. doi:10.1177/0266382116650792

Burgess, S. (2016). Representing small business web presence content: The web presence pyramid model. *European Journal of Information Systems*, *25*, 110–130. doi:10.1057/ejis.2015.4

Burhan, M., Rehman, R., Khan, B., & Kim, B. (2018). IoT elements, layered architectures, and security issues. *Sensors*, *18*(9), 27–96. doi:10.3390/s18092796

Burkholder, C., & MacEntee, K. (2016). Exploring the ethics of the participant-produced archive: The complexities of dissemination. *Ethics and Visual Research Methods*, 211–224. doi:10.1057/978-1-137-54305-9_16

Campbell, C. C. (2019). Solutions for counteracting human deception in social engineering attacks. *Information Technology & People, 32*, 1130–1152. doi:10.1108/itp-12-2017-0422

Cardoso, C. L., Gontijo, L. A., & Ono, M. M. (2017). Affective memory: An ethnographic approach to design. *Strategic Design Research Journal*, *10*, 79–88. doi:10.4013/sdrj.2017.101.09

Carias, J. F., Labaka, L., Sarriegi, J. M., & Hernantes, J. (2019). Defining a cyber resilience investment strategy in an industrial internet of things context. *Sensors*, *19*, 138–154. doi:10.3390/s19010138

Castillo-Montoya, M. (2016). Preparing for interview research. *The Qualitative Report*, *21*, 811–83. Retrieved from https://nsuworks.nova.edu/tqr/vol21/iss5/2

Ceric, A. (2016). Analysis of interactions between IT and organizational resources in a manufacturing organization using cross-impact analysis. *Journal of Enterprise Information Management*, *29*, 589–611. doi:10.1108/jeim-04-2015-0027

Cezar, A., Cavusoglu, H., & Raghunathan, S. (2017). Sourcing information security operations: The role of risk interdependency and competitive externality in outsourcing decisions. *Production and Operations Management*, *26*, 860–879. doi:10.1111/poms.12681

Chalvatzis, I., Karras, D. A., & Papademetriou, R. C. (2019). Evaluation of security vulnerability scanners for small and medium enterprises business networks resilience towards risk assessment. *2019 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA).* doi:10.1109/icaica.2019.8873438

Chen, R. (2019). Data breach on consumer behavior. *International Journal of Organizational and Collective Intelligence*, *9*(4), 1–17. doi:10.4018/ijoci.2019100101

Cheng, L., Liu, F., & Yao, D. D. (2017). Enterprise data breach: Causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *7*, 1942–4787. doi:10.1002/widm.1211

Choi, B. C., Kim, S. S., & Jiang, Z. (2016). Influence of firm's recovery endeavors upon privacy breach on online customer behavior. *Journal of Management Information Systems*, *33*, 904–933. doi:10.1080/07421222.2015.1138375

Choras, M., & Kozik, R. (2015). Machine learning techniques applied to detect cyber attackss on web applications. *Logic Journal of IGPL*, *23*(1), 45–56. doi:10.1093/jigpal/jzu038

City of Fort Lauderdale. (2018). City of Fort Lauderdale. *Business Tax*. Retrieved from https://www.fortlauderdale.gov/departments/finance/business-tax

Clark, K. R., & Veale, B. L. (2018). Strategies to enhance data collection and analysis in qualitative research. *Radiologic technology*, *89*, 482–485. Retrieved from http://www.radiologictechnology.org/content/89/5/482CT.extract

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*, 588–608. doi:10.2307/2094589

Collingridge, D. S., & Gantt, E. E. (2019). Republished: The Quality of qualitative research. *American Journal of Medical Quality, 34*, 439-445. doi:10.1177/1062860619873187

Connelly, L. M. (2016). Understanding research. Trustworthiness in qualitative research. *MEDSURG Nursing*, *25*, 435–436. Retrieved from https://www.medsurgnursing.net/archives/16nov/435

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

Costante, E., Fauri, D., Etalle, S., den Hartog, J., & Zannone, N. (2016). A hybrid framework for data loss prevention and detection. 2016 IEEE Security and Privacy Workshops (SPW), Security and Privacy Workshops (SPW), *2016 IEEE*, 324–333. doi:10.1109/SPW.2016.24

Cox, N., & Pilbauer, J. (2018). Outsourcing critical financial system operations. *Journal of Business Continuity & Emergency Planning*, *11*, 202–210. Retrieved from https://europepmc.org/abstract/med/29592820

Cumyn, A., Ouellet, K., Cote, A., Francoeur, C., & St-Onge, C. (2018). Role of researchers in the ethical conduct of research: A discourse analysis from different stakeholder perspectives. *Ethics & Behavior, 29,* 621–636. doi:10.1080/10508422.2018.1539671

Cypress, B. (2018). Qualitative research methods. *Dimensions of Critical Care Nursing*, *37*, 302–309. doi:10.1097/dcc.0000000000000322

Dai, J. (2018). Situation awareness-oriented cybersecurity education. *2018 IEEE Frontiers in Education Conference (FIE)*. *1*, 1–8 doi:10.1109/fie.2018.8658929

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

DeJonckheere, M., & Vaughn, L. M. (2019). Semistructured interviewing in primary care research: A balance of relationship and rigour. *Family Medicine and Community Health*, 7(2), 1–8. doi:10.1136/fmch-2018-000057

Denley, A., Foulsham, M., & Hitchen, B. (2019). GDPR principles. *GDPR – How to Achieve and Maintain Compliance*, 15–18. doi:10.4324/9780429449970-3

Densham, B. (2015). Three cyber-security strategies to mitigate the impact of a data breach. *Network Security*, *2015*(1), 5–8. doi:10.1016/s1353-4858(15)70007-3

De Oliveira Albuquerque, R., Garcia Villalba, L. J., Sandoval Orozco, A. L., De Sousa Junior, R. T., & Kim, T. (2016). Leveraging information security and computational trust for cybersecurity. *The Journal of Supercomputing*, *72*, 3729–3763. doi:10.1007/s11227-015-1543-4

Dhawase, S. G., Chaudhari, B. J., Kolambe, N. S., & Masare, P. S. (2018). Data leakage detection and prevention of confidential data. *International Journal of Computer Sciences and Engineering*, *6*, 213–218. doi:10.26438/ijcse/v6i6.213218

DHEW. (1979). The belmont report: Ethical principles and guidelines for the protection of human subjects of research: Appendix volume II. *PsycEXTRA Dataset*. Retrieved from https://archive.org/details/belmontreporteth00unit

Drechsler, A., & Weibschadel, S. (2018). An IT strategy development framework for small and medium enterprises. *Information Systems and e-Business Management*, *16*(1), 93–124. doi:10.1007/s10257-017-0342-2

Eddolls, M. (2016). Making cybercrime prevention the highest priority. *Network Security*, *2016*(8), 5–8. doi:10.1016/s1353-4858(16)30075-7

Elifoglu, I. H., Abel, I., & Tasseven, O. (2018). Minimizing insider threat risk with behavioral monitoring. *Review of business*, *38*, 61–73. Retrieved from https://www.stjohns.edu/academics/schools/peter-j-tobin-college-business/departments-faculty/review-business-interdisciplinary-journal-risk-and-society

Elman, C., Gerring, J., & Mahoney, J. (2016). Case study research: Putting the quant into the qual. *Sociological Methods & Research*, *45*, 375–391. doi:10.1177/0049124116644273

Englander, M. (2019). Phenomenological psychological interviewing. *The Humanistic Psychologist*. doi:10.1037/hum0000144

FBI. (2014). Internet crime complaint center. *2014 Internet Crime Report*. Retrieved from https://www.ic3.gov/media/annualreports.aspx

FBI. (2015). Internet crime complaint center. *2015 Internet Crime Report*. Retrieved from https://www.ic3.gov/media/annualreports.aspx

FBI. (2016a). *Cybercrime*. Retrieved from https://www.fbi.gov/investigate/cyber

FBI. (2016b). Internet crime complaint center. *2016 Internet Crime Report*. Retrieved from https://www.ic3.gov/media/annualreports.aspx

Feller, A., Mealli, F., & Miratrix, L. (2017). Principal score methods: Assumptions, extensions, and practical considerations. *Journal of Educational and Behavioral Statistics*, *42*, 726–758. doi:10.3102/1076998617719726

Fisher, R., Norman, M., & Klett, M. (2017). Enhancing infrastructure resilience through business continuity planning. *Journal of Business Continuity & Emergency Planning*, *11*, 163–173. Retrieved from https://www.ncbi.nlm.nih.gov/pubmed/29256383

Flynn, S. V., & Korcuska, J. S. (2018). Credible Phenomenological Research: A Mixed-Methods Study. *Counselor Education and Supervision, 57*(1), 34-50. doi:10.1002/ceas.12092

Gajic, S., Palcic, I., & Cosic, I. (2015). Complexity perspective and engineering systems: Novel approaches. *DAAAM Proceedings*, *26*, 1091–1096. doi:10.2507/26th.daaam.proceedings.153

Galinec, D., Moznik, D., & Guberina, B. (2017). Cybersecurity and cyber defence: National level strategic approach. *Automatika: Journal for Control, Measurement, Electronics, Computing & Communications*, *58*, 273–286. doi:10.1080/00051144.2017.1407022

Gallin, J. I., Ognibene, F. P., & Johnson, L. L. (2017). *Principles and Practice of Clinical Research* (4th ed.). Retrieved from https://www.elsevier.com/books/principles-and-practice-of-clinical-research/gallin/978-0-12-849905-4

Gangwar, H., & Date, H. (2016). Understanding cloud computing adoption: A model comparison approach. *Human Systems Management*, *35*, 93–114. doi:10.3233/hsm-150857

George, G., & Thampi, S. M. (2019). Vulnerability-based risk assessment and mitigation strategies for edge devices in the Internet of Things. *Pervasive and Mobile Computing, 59*. doi:10.1016/j.pmcj.2019.101068

Gil, D., Ferrandez, A., Mora-Mora, H., & Peral, J. (2016). Internet of things: A review of surveys based on context-aware intelligent services. *Sensors*, *16*, 1069. doi:10.3390/s16071069

Goldsborough, R. (2016). Protecting yourself from ransomware. *Google Hacking for Penetration Testers*, *43*, 70–71. Retrieved from http://www.teacherlibrarian.com/

Gonzalez-Saldivar, G., Rodriguez-Gutierrez, R., Viramontes-Madrid, J. L., Salcido-Montenegro, A., Alvarez-Villalobos, N. A., Gonzalez-Nava, V., & Gonzalez-Gonzalez, J. G. (2019). Participants' awareness of ethical compliance, safety and protection during participation in pharmaceutical industry clinical trials: a controlled survey. *BMC Medical Ethics, 20*(1), 1–10. doi:10.1186/s12910-018-0344-8

Goode, S., Hoehle, H., Venkatesh, V., & Brown, S. A. (2017). User compensation as a data breach recovery action: An investigation of the Sony PlayStation network breach. *MIS Quarterly*, *41*, 703–727. doi:10.25300/misq/2017/41.3.03

Greater Fort Lauderdale. (2018). Ft. Lauderdale chamber of commerce. *networking and development*. Retrieved from https://www.ftlchamber.com/

Greenacre, J. (2015). The roadmap approach to regulating digital financial services. *Journal of Financial Regulation*, *1*, 298–305. doi:10.1093/jfr/fjv008

Griffith, D. A., Morris, E. S., & Thakar, V. (2016). Spatial autocorrelation and qualitative sampling: The case of snowball type sampling designs. *Annals of the American Association of Geographers*, *106*, 773–787. doi:10.1080/24694452.2016.1164580

Gross, M. L., Canetti, D., & Vashdi, D. R. (2017). Cyberterrorism: Its effects on psychological well-being, public confidence and political attitudes. *Journal of Cybersecurity*, *3*, 49–58. doi:10.1093/cybsec/tyw018

Guitton, C. (2017). Foiling cyber attacks. *2017 International Conference on Cyber Security And Protection Of Digital Services (Cyber Security)*. doi:10.1109/cybersecpods.2017.8074853

Gutierrez-Martinez, J., Nunez-Gaona, M. A., & Aguirre-Meneses, H. (2015). Business model for the security of a large-scale PACS, compliance with ISO/27002:2013 standard. *Journal of Digital Imaging*, *28*, 481–491. doi:10.1007/s10278-014-9746-4

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, *3*, 1–18. doi:10.1016/j.heliyon.2017.e00346

Heale, R., & Twycross, A. (2017). What is a case study? *Evidence Based Nursing*, *21*(1), 7-8. doi:10.1136/eb-2017-102845

Heller, R., Toregas, C., & Hoffman, L. (2019). Reach to teach: Preparing cybersecurity experts as adjunct community college faculty. *Proceedings of the 11th*

International Conference on Computer Supported Education, 338–343. doi:10.5220/0007612603380343

Hennig, N. (2018). Privacy and security online: Best practices for cybersecurity. *Library Technology Reports*, *54*, 1–37. Retrieved from https://journals.ala.org/index.php/ltr/article/viewFile/6634/8889

Henry, S., & Ali, M. L. (2017). Cloud computing security threats and solutions. I-*manager's Journal on Cloud Computing, 4*(2), 1–8. doi:10.26634/jcc.4.2.14249\

Holland, C. P., & Gutierrez-Leefmans, M. (2018). A taxonomy of SME e-commerce platforms derived from a market-level analysis. *International Journal of Electronic Commerce*, *22*, 161–201. doi:10.1080/10864415.2017.1364114

Howell, V. W. (2016). Developing cybersecurity training. *Ceramic Industry, 166*, 19–22. Retrieved from http://it4sec.org/article/levels-cybersecurity-training-and-education.

Huang, K., Siegel, M., & Madnick, S. (2018). Systematically understanding the cyber attacks business: A survey. *ACM Computing Surveys*, *51*, 1–36. doi:10.1145/3199674

Hunter, A. (2017). Interviews in qualitative research. *Qualitative Methods and Health Policy Research,* 76–102. doi:10.4324/9781315127873-5

Iovan, S., & Iovan, A. (2016). From cyber threats to cyber-crime. *Journal of Information Systems & Operations Management*, *10*, 425–434. Retrieved from http://jisom.rau.ro

Irons, A. (2019). Delivering cybersecurity education effectively. *Cybersecurity Education for Awareness and Compliance,* 135–157. doi:10.4018/978-1-5225-7847-5.ch008

Izuakor, C. (2016). Understanding the impact of cybersecurity risks on safety. *Proceedings of the 2nd International Conference on Information Systems Security and Privacy*, *1*, 509–513. doi:10.5220/0005796805090513

Jacobs, T., & Tschotschel, R. (2019). Topic models meet discourse analysis: A quantitative tool for a qualitative approach. *International Journal of Social Research Methodology, 22,* 469–485. doi:10.1080/13645579.2019.1576317

James, L. (2018). Making cyber-security a strategic business priority. *Network Security*, *8*(5), 6–8. doi:10.1016/S1353-4858(18)30042-4

Janakiraman, R., Lim, J. H., & Rishika, R. (2018). The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. *Journal of Marketing*, *82*, 85–105. doi:10.1509/jm.16.0124

Janecek, V. (2018). Ownership of personal data in the internet of things. *Computer Law & Security Review*, *34*, 1039–1052. doi:10.1016/j.clsr.2018.04.007

Jenab, K., & Moslehpour, S. (2016). Cybersecurity management. *Business Management Dynamics*, *5*(11), 16–39. Retrieved from http://bmdynamics.com/issue_pdf/bmd110587-%2016-39

Jia, Y., Qi, Y., Shang, H., Jiang, R., & Li, A. (2018). Research cybersecurity—article: A practical approach to constructing a knowledge graph for cybersecurity. *Engineering*, *4*(1), 53–60. doi:10.1016/j.eng.2018.01.004

Jones, J., & Shashidhar, N. (2017). Ransomware analysis and defense: WannaCry and the Win32 environment. *International Journal of Information Security Science*, *6*, 57–69. Retrieved from http://www.ijiss.org/ijiss/index.php/ijiss/article/view/257

Joo, J., & Hovav, A. (2016). The influence of information security on the adoption of web-based integrated information systems: An e-government study in Peru. *Information Technology for Development*, *22*, 94–116. doi:10.1080/02681102.2014.979393

Kadir, N. K., Judhariksawan, J., & Maskun, M. (2019). Terrorism and cyberspace: A phenomenon of cyber-terrorism as transnational crimes. *Fiat Justisia, 13,* 333–344. doi:10.25041/fiatjustisia.v13no4.1735

Kafol, C., & Bregar, A. (2017). Cybersecurity-Building a sustainable protection. *DAAAM International Scientific Book*, 081–090. doi:10.2507/daaam.scibook.2017.07

Kalaiprasath, R., Elankavi, R., & Udayakumar, R. (2017). Cloud security and compliance - a semantic approach in end to end security. *International Journal on Smart Sensing & Intelligent Systems, 10*, 482–494. doi:10.21307/ijssis-2017

Kaur, K., Gupta, I., & Singh, A. K. (2017). A comparative evaluation of data leakage/loss prevention systems (DLPS). *Computer Science & Information Technology (CS & IT)*, *9*, 87–95. doi:10.5121/csit.2017.71008

Kaushik, K., Kumar Jain, N., & Kumar Singh, A. (2018). Antecedents and outcomes of information privacy concerns: Role of subjective norm and social presence. *Electronic Commerce Research and Applications, 32,* 57–68. doi:10.1016/j.elerap.2018.11.003

Kesan, J. P., & Hayes, C. M. (2017). Strengthening cybersecurity with cyber insurance markets and better risk assessment. *Minnesota Law Review,120*, 191–276. Retrieved from https://minnesotalawreview.org/article/strengthening-cybersecurity/

Kim, B., Johnson, K., & Park, S. (2017). Lessons from the five data breaches: Analyzing framed crisis response strategies and crisis severity. *Cogent Business & Management*, *4*(1), 1–15. doi:10.1080/23311975.2017.1354525

Kim, H., Lee, D., & Ryu, M. (2018). An optimal strategic business model for small businesses using online platforms. *Sustainability*, *10*, 500–579. doi:10.3390/su10030579

King, Z. M., Henshel, D. S., Flora, L., Cains, M. G., Hoffman, B., & Sample, C. (2018). Characterizing and measuring maliciousness for cybersecurity risk assessment. *Frontiers in Psychology, 9.* doi:10.3389/fpsyg.2018.00039

Korstjens, I., & Moser, A. (2017). Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing. *European Journal of General Practice*, *24*, 120–124. doi:10.1080/13814788.2017.1375092

Korte, J. (2017). Mitigating cyber risks through information sharing. *Journal of Payments Strategy & Systems*, *11*, 203–214. Retrieved from https://www.ingentaconnect.com/content/hsp/jpss/2017/00000011/00000003/art00005

Krunal, G., & Viral, P. (2017). Survey on ransomware: A new era of cyber attacks. International *Journal of Computer Applications, 168*, 38–41. doi:10.5120/ijca2017914446

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

Lei, M., Yang, Y., Niu, X., Yang, Y., & Hao, J. (2017). An overview of general theory of security. *China Communications*, *14*(7), 1-10. doi:10.1109/cc.2017.8010961

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, *37*, 263–280. doi:10.1080/01639625.2015.1012409

Li, W., Liu, K., Belitski, M., Ghobadian, A., & O'Regan, N. (2016). E-Leadership through strategic alignment: An empirical study of small and medium-sized enterprises in the digital age. *Journal of Information Technology*, *31*, 185–206. doi:10.1057/jit.2016.10

Lopes, I. M., & Oliveira, P. (2016). Adoption of an information systems security policy in small and medium sized enterprises. *Journal of Information Systems Engineering & Management*, *1*(1), 3-13. doi:10.20897/lectito.201605

Ma, Z. (2017). CPSec DLP: kernel-level content protection security system of data leakage prevention. *Chinese Journal of Electronics, 26*, 827–2836. doi:10.1049/cje.2017.05.002

Maguire, M., & Delahunt, B. (2017). Doing a thematic analysis: A practical, step-by-step guide for learning and teaching scholars. *AISHE-J: The All Ireland Journal of Teaching & Learning in Higher Education*, *9*, 3351. Retrieved from http://ojs.aishe.org/index.php/aishe-j/article/viewFile/335/553

Makridis, C., & Dean, B. (2018). Measuring the economic effects of data breaches on firm outcomes: Challenges and opportunities. *Journal of Economic and Social Measurement*, *43*, 59–83. doi:10.3233/jem-180450

Mann, S. (2016). Qualitative interviews overview. *The Research Interview*, *1*, 30–57. doi:10.1057/9781137353368_2

Marti, K. (2015). Stochastic optimal open-loop feedback control. *Stochastic Optimization Methods*, 79–118. doi:10.1007/978-3-662-46214-0_3

Mermigas, D., & Pirounias, S. (2018). Formal quantification of information systems' security and estimation of the cost of breaches. 2018 International Conference on Sensor Networks and Signal Processing (SNSP), Sensor Networks and Signal Processing (SNSP), *2018 International Conference on, SNSP,* 130–138. doi:10.1109/SNSP.2018.00033

Meyers, J. J., Hansen, D. L., Giboney, J. S., & Rowe, D. C. (2018). Training future cybersecurity professionals in spear-phishing using SiEVE. *Proceedings of the 19th Annual SIG Conference on Information Technology Education - SIGITE '18*. 135–140. doi:10.1145/3241815.3241871

Meyvis, T., & Van Osselaer, S. M. (2017). Increasing the power of your study by increasing the effect size. *Journal of Consumer Research*, *44*, 1157–1173. doi:10.1093/jcr/ucx110

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

Mokwena, S., & Hlebela, C. (2018). Factors affecting the adoption of software as a service in South African Small Medium enterprises. *2018 Open Innovations Conference (OI), Open Innovations Conference (OI), 2018*, 1–6. doi:10.1109/OI.2018.8535714

Monat, J., & Gannon, T. (2018). Applying systems thinking to engineering and design. *Systems, 6(3),* 34. doi:10.3390/systems6030034

Moore, T. (2017). On the harms arising from the Equifax data breach of 2017. *International Journal of Critical Infrastructure Protection*, *19*, 47–48. doi:10.1016/j.ijcip.2017.10.004

Motoyama, Y., & Mayer, H. (2017). Revisiting the roles of the university in regional economic development: A triangulation of data. *Growth and Change*, *48*, 787–804. doi:10.1111/grow.12186

Munier, L., & Kemball-Cook, A. (2019). Blockchain and the general data protection regulation: Reconciling protection and innovation. *Journal of Securities Operations & Custody, 11*, 145–157. Retrieved from

https://www.ingentaconnect.com/content/hsp/jsoc/2019/00000011/00000002/art00005

Muronga, K., Herselman, M., Botha, A., & Da Veiga, A. (2019). An analysis of assessment approaches and maturity scales used for evaluation of information security and cybersecurity user awareness and training programs: A scoping review. *2019 Conference on Next Generation Computing Applications (NextComp), Next Generation Computing Applications (NextComp), 2019 Conference On*, 1–6. doi:10.1109/NEXTCOMP.2019.8883535

Nastasiu, C. (2016). Cybersecurity strategies in the Internet era. *Proceedings of the Scientific Conference AFASES, 2*, 619–624. doi:10.19062/22473173.2016.18.2.19

Naudet, Y., Mayer, N., & Feltus, C. (2016). Towards a systemic approach for information security risk management. *2016 11th International Conference on Availability, Reliability and Security (ARES)*, 177–186. doi:10.1109/ares.2016.76

Nelson, J. (2016). Using conceptual depth criteria: Addressing the challenge of reaching saturation in qualitative research. *Qualitative Research, 17*, 554–570. doi: 10.1177/1468794116679873

Nicola, F. (2018). The internet of things ecosystem: The blockchain and data protection issues. *Advances in Science, Technology and Engineering Systems Journal*, *3*(2), 1–7. doi:10.25046/aj030201

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

Information Systems, *8*(1), 42–63. Retrieved from https://digitalcommons.kennesaw.edu/ajis/vol8/iss1/3/

Ogunshile, E. K. (2018). Leveraging cloud computing, virtualization and solar technologies to increase performance and reduce cost in small to medium-sized businesses. *Proceedings of the 8th International Conference on Cloud Computing and Services Science*, *1*, 310–321. doi:10.5220/0006641103100321

Oltmann, S. (2016). Qualitative interviews: A methodological discussion of the interviewer and respondent contexts. *Qualitative Social Research*, *17*, 2–15. Retrieved from http://www.qualitative-research.net/index.php/fqs/article /view/2551/3998

Onwubiko, C. (2017). Security operations centre: Situation awareness, threat intelligence and cybercrime. *2017 International Conference on Cyber Security and Protection Of Digital Services (Cyber Security)*, 1–6. doi:10.1109/cybersecpods.2017.8074844

Opitz, E. L. (2018). Cybersecurity for the board of directors of small and midsized businesses. Board Leadership, *2018(159),* 4–5. doi:10.1002/bl.30115

Paliszkiewicz, J. (2019). Information security policy compliance: Leadership and trust. *Journal of Computer Information Systems*, *59*, 211–217. doi:10.1080/08874417.2019.1571459

Pan, Y., White, J., & Sun, Y. (2016). Assessing the threat of web worker distributed attacks. *2016 IEEE Conference on Communications and Network Security (CNS)*, 306–314. doi:10.1109/cns.2016.7860498

Pantangi, A., Xiong, K., & Makati, M. (2016). SECUPerf: End-to-end security and performance assessment of cloud services. *2016 IEEE Trustcom/BigDataSE/ISPA*, 405–410. doi:10.1109/trustcom.2016.0268

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

Parks, R. F., & Adams, L. (2016). Analyzing security breaches in the U.S.: A business analytics case-study. *Information Systems Education Journal*, *14*, 43–48. Retrieved from http://isedj.org/2016-14/n2/ISEDJv14n2p43.html

Paulus, T., Woods, M., Atkins, D. P., & Macklin, R. (2017). The discourse of QDAS: reporting practices of ATLAS.ti and NVivo users with implications for best practices. *International Journal of Social Research Methodology*, *20*(1), 35–47. doi:10.1080/13645579.2015.1102454

Peticca-Harris, A., DeGama, N., & Elias, S. R. (2016). A dynamic process model for finding informants and gaining access in qualitative research. *Organizational Research Methods*, *19*, 376–401. doi:10.1177/1094428116629218

Phillippi, J. G., & Lauderdale, J. (2017). A guide to field notes for qualitative research: Context and conversation. *Qualitative Health Research*, *28*, 381–388. doi:10.1177/1049732317697102

Plachkinova, M., & Maurer, C. (2018). Teaching case security breach at Target. *International Journal of Information Privacy, Security and Integrity*, *29*, 11–19. Retrieved from http://jise.org/Volume29/n1/JISEv29n1p11.html

Prince, D. (2018). Cybersecurity: The security and protection challenges of our digital world. *Computer, 51*, 16–19. doi:10.1109/MC.2018.2141025

Rahman, M. T., Rahman, M. S., Wang, H., Tajik, S., Khalil, W., Farahmandi, F., … Tehranipoor, M. (2019). Defense-in-depth: A recipe for logic locking to prevail. *Integration*. doi:10.1016/j.vlsi.2019.12.007

Reinecke, J., Arnold, D. G., & Palazzo, G. (2016). Qualitative methods in business ethics, corporate responsibility, and sustainability research. *Business Ethics Quarterly, 26*, 13-22. doi:10.1017/beq.2016.67

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

Reyns, B. W. (2015). A routine activity perspective on online victimisation. *Journal of Financial Crime*, *22*, 396–411. doi:10.1108/jfc-06-2014-0030

Riahi Sfar, A., Natalizio, E., Challal, Y., & Chtourou, Z. (2018). A roadmap for security challenges in the Internet of Things. *Digital Communications and Networks*, *4*, 118–137. doi:10.1016/j.dcan.2017.04.003

Richardson, R., & North, M. (2017). Ransomware: Evolution, mitigation, and prevention. *International Management Review*, *13*, 10–21. Retrieved from https://www.questia.com/library/journal/1P3-4321221657/ransomware-evolution-mitigation-and-prevention

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

Rizov, V. (2018). Information sharing for cyber threats. *Information & Security: An International Journal*, *39*(1), 43–50. doi:10.11610/isij.3904

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

Ronchi, A. M. (2019). Fostering the culture of cyber security. 2019 IST-Africa Week Conference (IST-Africa), *IST-Africa Week Conference (IST-Africa), 2019*, 1–10. doi:10.23919/ISTAFRICA.2019.8764870.

Roseveare, J. (2017). A practitioner's viewpoint: Limitations and assumptions implicit in assessment. *Psychometric Testing*, 251-261. doi:10.1002/9781119183020.ch18

Rothrock, R. A., Kaplan, J., & Van, D. O. (2018). The board's role in managing cybersecurity risks. *MIT Sloan Management Review, 59*(2), 12–15. Retrieved from https://sloanreview.mit.edu/

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

Sabillon, R., Cavaller, V., Cano, J., & Serra-Ruiz, J. (2016). Cybercriminals, cyberattacks and cybercrime. *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, 1–9. doi:10.1109/icccf.2016.7740434

Sabitha, S., & Rajasree, M. (2017). Access control-based privacy-preserving secure data sharing with hidden access policies in cloud. *Journal of Systems Architecture, 75*, 50–58. doi:10.1016/j.sysarc.2017.03.002

Sandberg, B. (2019). Art hacking for business innovation: An exploratory case study on applied artistic strategies. *Journal of Open Innovation, 5*(1), 20. doi:10.3390/joitmc5010020

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

Savard, D. M. (2018). A routine activity approach: Assessing victimization by gender in transit environments and other public locations. *Advances in Applied Sociology*, *8*(1), 56–75. doi:10.4236/aasoci.2018.81004

SBA. (2018a). Small business size standards: *Size standards methodology white paper*. Retrieved from https://www.sba.gov/document/support--size-standards-methodology-white-paper

SBA. (2018b). South Florida district office: *The U.S. small business administration SBA.gov*. Retrieved from https://www.sba.gov/offices/district/fl/miami

Schabacker, D. S., Levy, L., Evans, N. J., Fowler, J. M., & Dickey, E. A. (2019). Assessing cyberbiosecurity vulnerabilities and infrastructure resilience. *Frontiers in Bioengineering and Biotechnology, 7*, 61. doi:10.3389/fbioe.2019.00061

Schulz, G. (2019). Data infrastructure availability, data protection, security, and strategy. *Data Infrastructure Management,* 87–122. doi:10.1201/9780429264955-6

Selznick, L. F., & Lamacchia, C. (2018). Cybersecurity liability: How technically savvy can we expect small business owners to be? *Journal of Business & Technology Law*, *13*, 217–253. Retrieved from https://ssrn.com/abstract=3200021

Senarathna, I., Yeoh, W., Warren, M., & Salzman, S. (2016). Security and privacy concerns for Australian SMEs cloud adoption: Empirical study of metropolitan vs regional SMEs. *Australasian Journal of Information Systems, 20*, 1–20. doi:10.3127/ajis.v20i0.1193

Sharma, G., & Lijuan, W. (2015). The effects of online service quality of e-commerce websites on user satisfaction. *The Electronic Library*, *33*, 468–485. doi:10.1108/el-10-2013-0193

Sobitha Ahila, S., & Shunmuganathan, K. L. (2016). Role of agent technology in web usage mining: Homomorphic encryption-based recommendation for E-commerce applications. *Wireless Personal Communications*, *87*, 499–512. doi:10.1007/s11277-015-3082-y

Sollars, M. (2016). Risk-based security: Staff can play the defining role in securing assets. *Network Security, 2016*, 9–12. doi:10.1016/s1353-4858(16)30087-3

Soulier, A. (2019). Reconsidering dynamic consent in biobanking: Ethical and political consequences of transforming research participants into ICT users. IEEE Technology and Society Magazine, *Technology and Society Magazine, IEEE, IEEE Technol. Soc. Mag, 38,* 62–70. doi:10.1109/MTS.2019.2913072

Stanciu, V., & Tinca, A. (2017). Exploring cybercrime – realities and challenges. *Journal of Accounting and Management Information Systems*, *16*, 610–632. doi:10.24818/jamis.2017.04009

Stitilis, D., Pakutinskas, P., Kinis, U., & Malinauskaite, I. (2016). Concepts and principles of cybersecurity strategies. *Journal of Security & Sustainability Issues*, *6*, 197–210. doi:10.9770/jssi.2016.6.2(1)

Sultan, H., Khalique, A., Alam, S. I., & Tanweer, S. (2018). A survey on ransomware: Evolution, growth, and impact. *International Journal of Advanced Research in Computer Science*, *9*, 802–810. Retrieved from http://www.ijarcs.info/index.php/Ijarcs/article/view/5858

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

Talesh, S. A. (2018). Data breach, privacy, and cyber insurance: How insurance companies act as compliance managers for businesses. *Law & Social Inquiry*, *2,* 417. Retrieved from https://onlinelibrary.wiley.com/doi/abs/10.1111/lsi.12303

Tasevski, P. (2016). Cyber awareness, strategies, and practice. *Information & Security: An International Journal*, *34*, 5–6. doi:10.11610/isij.3400

Terlizzi, M. A., Meirelles, F. S., & Viegas Cortez da Cunha, M. A. (2017). Behavior of Brazilian banks employees on Facebook and the cybersecurity governance. *Journal of Applied Security Research, 12*, 224–252. doi:10.1080/19361610.2017.1277886

Terzi, M. (2019). E-government and cyber terrorism: Conceptual framework, theoretical discussions, and possible solutions. *Tesam Akademi Dergisi, 6*, 213–247. doi:10.30626/tesamakademi.528011

Thomas, D. R. (2016). Feedback from research participants: Are member checks useful in qualitative research? *Qualitative Research in Psychology*, *14*(1), 23–41. doi:10.1080/14780887.2016.1219435

Thomas, J. E., & Galligher, G. C. (2018). Improving backup system evaluations in information security risk assessments to combat ransomware. *Computer and Information Science*, *11*(1), 14–25. doi:10.5539/cis.v11n1p14

Tibben, W. J. (2015). Theory building for ICT4D: Systemizing case study research using theory triangulation. *Information Technology for Development*, *21*, 628–652. doi:10.1080/02681102.2014.910635

Tisdale, S. M. (2015). Cybersecurity: Challenges from a system, complexity, knowledge management and business intelligence perspective. *Issues in Information Systems*, *16*, 191–198. Retrieved from http://www.iacis.org/iis/2015/3_iis_2015_191-198

Trappe, W., & Straub, J. (2018). Journal of cybersecurity and privacy: A new open access journal. *Journal of Cybersecurity and Privacy*, *1*(1), 1-3. doi:10.3390/jcp1010001

Tu, C., Yuan, Y., Archer, N., & Connelly, C. (2018). Strategic value alignment for information security management: A critical success factor analysis. *Information & Computer Security*, *26*, 150–170. doi:10.1108/ICS-06-2017-0042

Twycross, A., & Shorten, A. (2016). Using observational research to obtain a picture of nursing practice: Table 1. *Evidence Based Nursing*, *19*(3), 66–67. doi:10.1136/eb-2016-102393

Udroiu, A. M. (2018). Implementing the cybersecurity awareness program using elearning platform. *eLearning & Software for Education, 4*, 101–104. doi:10.12753/2066-026X-18-229

Valerio, M. A., Rodriguez, N., Winkler, P., Lopez, J., Dennison, M., Liang, Y., & Turner, B. J. (2016). Comparing two sampling methods to engage hard-to-reach communities in research priority setting. *BMC Medical Research Methodology*, *16*(1), 1–11. doi:10.1186/s12874-016-0242-z

Van de Weijer, S. G., & Leukfeldt, E. R. (2017). Big five personality traits of cybercrime victims. *Cyberpsychology, Behavior, and Social Networking*, *20*, 407–412. doi:10.1089/cyber.2017.0028

Van de Wiel, M. (2017). Examining expertise using interview and verbal protocols. *Frontline Learning Research*, *5*(3), 112–140. doi:10.14786/flr.v5i3.257

Van Hilten, A. (2018). A novice reflects on the research interview: Reflective practice and reflexivity in research processes a novice reflects on the research interview. *Qualitative Research in Organizations and Management: An International Journal*, *13*, 121–122. doi:10.1108/qrom-10-2016-1447

Vavilis, S., Petkovic, 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

Vlad-Mihai, C. (2017). Insider threat detection and mitigation techniques. *Scientific Bulletin of Naval Academy,1*. 379–381. doi:10.21279/1454-864X-17-I1-060

Von Bertalanffy, L. (1950). An outline of general system theory. *The British Journal for the Philosophy of Science*, *I*, 134–165. doi:10.1093/bjps/i.2.134

Von Bertalanffy, L. (1969). General system theory: Foundations, development, applications. *New York, NY: George Braziller*, *164*, 681–682. doi:10.1126/science.164.3880.681

Von Bertalanffy, L. (1972). The history and status of general system theory. *Academy of Management Journal*, *15*, 407–426. doi:10.5465/255139

Wadhwa, A., & Arora, N. (2017). A review on cybercrime: Major threats and solutions. *International Journal of Advanced Research in Computer Science*, *8*, 2217–2221. doi:10.26483/ijarcs.v8i5.4067

Wainwright, R. (2018). Fighting crime and terrorism in the age of technology. *Brown Journal of World Affairs, 24*, 191–203. Retrieved from http://bjwa.brown.edu/24-2/fighting-crime-and-terrorism-in-the-age-of-technology/

Wang, J., Shan, Z., Gupta, M., & Rao, H. R. (2019). A longitudinal study of unauthorized access attempts on information systems: The role of opportunity contexts. *MIS Quarterly*, *43*, 601–622. doi:10.25300/misq/2019/14751

Wang, Y., Shi, S., Nevo, S., Li, S., & Chen, Y. (2015). The interaction effect of IT assets and IT management on firm performance: A systems perspective. *International Journal of Information Management*, *35*, 580–593. doi:10.1016/j.ijinfomgt.2015.06.006

Watad, M., Washah, S., & Perez, C. (2018). IT security threats and challenges for small firms: Managers' perceptions. *International journal of the academic business*

world, *12*(1), 23–30. Retrieved from https://jwpress.com/Journals/IJABW/BackIssues/IJABW-Spring-2018.pdf#page=29

Weis, D., & Willems, H. (2017). Aggregation, validation, and generalization of qualitative data - methodological and practical research strategies illustrated by the research process of an empirically based typology. *Integrative Psychological and Behavioral Science, 2,* 223–243. doi:10.1007/s12124-016-9372-4

White, D., & Hind, D. (2015). Projection of participant recruitment to primary care research: A qualitative study. *Trials*, *16*(1), 473. doi:10.1186/s13063-015-1002-9

Williams, B., Bengert, A., & Ward-Caldwell, B. (2016). Hacked: A qualitative analysis of media coverage of the Sony breach. *iConference 2016 Proceedings*. doi:10.9776/16335

Williams, M. L. (2016). Guardians upon high: An application of routine activities theory to online identity theft in Europe at the country and individual level. *British Journal of Criminology*, *56*(1), 21–48. doi:10.1093/bjc/azv011

Williams, M. L., Levi, M., Burnap, P., & Gundur, R. (2018). Under the corporate radar: Examining insider business cybercrime victimization through an application of routine activities theory. *Deviant Behavior*, 1–13. doi:10.1080/01639625.2018.1461786

Wilson, V. (2016). Research methods: Design, methods, case study…oh my! *Evidence Based Library and Information Practice*, *11*(1), 39–40. doi:10.18438/b8h928

Wolff, J. (2016). Perverse effects in defense of computer systems: When more is less. *Journal of Management Information Systems*, *33*, 597–620. doi:10.1080/07421222.2016.1205934

Yaqoob, I., Ahmed, E., Rehman, M. H., Ahmed, A. I., Al-garadi, M. A., Imran, M., & Guizani, M. (2017). The rise of ransomware and emerging security challenges in the Internet of Things. *Computer Networks*, *129*, 444–458. doi:10.1016/j.comnet.2017.09.003

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

You, Y., Oh, J., Kim, S., & Lee, K. (2018). Advanced approach to information security management system utilizing maturity models in critical infrastructure. *KSII Transactions on Internet and Information Systems,* 49–95. doi:10.3837/tiis.2018.10.020

Young, C. S. (2016). Information security threats and risk. *Information Security Science*, 3–27. doi:10.1016/b978-0-12-809643-7.00001-2

Yuhuan, Q. (2017). Cloud storage technology. *Big Data and Cloud Innovation, 1*(1). doi:10.18063/bdci.v1i1.508

Zamawe, F. (2015). The implication of using NVivo software in qualitative data analysis: Evidence-based reflections. *Malawi Medical Journal*, *27*(1), 13–15. doi:10.4314/mmj.v27i1.4

Appendix A: Interview Protocol / Observation Protocol

Project: Doctoral Study at Walden University

Type of Interview:_____

Date:_____

Place:_____

Interviewer:_____

Interviewee:_____

Interviewee Title:_____

What to do

1. Introduce the study project by explaining to the participant about (a) the purpose of the study, (b) data collection sources, (c) data confidentiality (d) and interview completion which will be less than one hour.
2. The participant will be provided with contact information and will be reminded of their consent to participate in the study
3. The digital audio recorder will be turned on to test the functionality of the device.
4. Throughout the interview, I will watch for non-verbal signals. Paraphrase text if needed. Ask probing questions and follow up to provide a more detailed understanding.
5. Thank participants for their support and contribution to the interview process. Recap the secrecy of responses from the participants.
6. Conclude the interview by thanking the participants and schedule a member checking follow-up to confirm the transcribe interview summary within a week of the

interview. By informing participants that they have to review, approval, and return the copy of the transcription file.

What to say:

I am Martins Idahosa; I appreciate your willingness and time to participate in this research today. As we discuss each interview question, kindly provide your experience and thoughts and feel free to clarify any asked questions.

1. Please describe the strategies and various security tools that your organizations currently utilize to address or mitigate targeted cyber attackss successfully?
2. How, if at all, do you conduct a security system assessment to ensure basic security practices are in place?
3. What successful processes have you implemented to implement your security awareness program?
4. What, if any, successful employee training have you implemented for security procedures to improve and enhance cyber attacks detection capabilities?
5. How successful is your response plan for detecting, preventing and protecting both business and consumers' data?
6. What is your contingency plan in the event of a successful cyber–attack?
7. What successful data control techniques have you implemented?
8. What else can you tell me regarding how your business is protecting customers' data against cyber–attacks?

Appendix B: Interview Questions for Cyber Security Strategies

1. Please describe the strategies and various security tools that your organizations currently utilize to address or mitigate targeted cyber attackss successfully?
2. How, if at all, do you conduct a security system assessment to ensure basic security practices are in place?
3. What successful processes have you implemented to implement your security awareness program?
4. What, if any, successful employee training have you implemented for security procedures to improve and enhance cyber attacks detection capabilities?
5. How successful is your response plan for detecting, preventing and protecting both business and consumers' data?
6. What is your contingency plan in the event of a successful cyber–attack?
7. What successful data control techniques have you implemented?
8. What else can you tell me regarding how your business is protecting customers' data against cyber–attacks?