


2017

Effective Cyber Security Strategies for Small Businesses

Kimberly Diane Cook
Walden University

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

 Part of the [Business Administration, Management, and Operations Commons](#), and the [Management Sciences and Quantitative Methods 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

Kimberly Cook

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. Julia East, Committee Chairperson, Doctor of Business Administration Faculty

Dr. Doron Zilbershtein, Committee Member, Doctor of Business Administration Faculty

Dr. Diane Dusick, University Reviewer, Doctor of Business Administration Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2017

Abstract

Effective Cyber Security Strategies for Small Businesses

by

Kimberly Diane Cook

MBA, Webster University, 2008

MS, National Louis University, 1996

BS, National Louis University, 1993

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

June 2017

Abstract

Disruptive technologies developed in the digital age expose individuals, businesses, and government entities to potential cyber security vulnerabilities. Through the conceptual framework of general systems theory, this multiple case study was used to explore the strategies among owners of 4 retail small- and medium-size enterprises (SMEs) in Melbourne, Florida, who successfully protected their businesses against cyber attacks. The data were collected from a review of archival company documents and semistructured interviews. Yin's 5-phased cycles for analyzing case studies provided the guidelines for the data analysis process. Three themes emerged from thematic analysis across the data sets: cyber security strategy, reliance on third-party vendors for infrastructure services, and cyber security awareness. The study findings indicated that the SME owners' successful cyber security strategies might serve as a foundational guide for others to assess and mitigate cyber threat vulnerabilities. The implications for positive social change include the potential to empower other SME owners, new entrepreneurs, and academic institutions with successful cyber security strategies and resources to affect changes within the community. SME owners who survive cyber attacks may spur economic growth by employing local residents, thus stimulating the socioeconomic lifecycle. Moreover, implementation of these successful strategies may catalyze consumer confidence, resulting in greater economic prosperity.

Effective Cyber Security Strategies for Small Businesses

by

Kimberly Diane Cook

MBA, Webster University, 2008

MS, National Louis University, 1996

BS, National Louis University, 1993

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

June 2017

Acknowledgments

First and foremost, I am grateful to God for giving me the strength and resources to succeed. Secondly, I would like to thank my twin daughters, Kylie and Kaitlin, and my mother, Susan, for their never-ending support, inspiration, and unwavering encouragement. Without their daily sacrifices, I would not have been able to achieve my lifelong dream. Finally, I want to thank my Walden DBA committee chair Dr. Julia East for her guidance, advocacy, and mentorship as I navigated through this arduous journey. I would be remiss if I did not also thank my other committee members Dr. Doron Zilbershtein and Dr. Diane Dusick for their meticulous oversight, patience, and support.

Table of Contents

List of Tables	v
List of Figures	i
Section 1: Foundation of the Study.....	1
Background of the Problem	2
Problem Statement	3
Purpose Statement.....	3
Nature of the Study	4
Research Question	6
Interview Questions	6
Conceptual Framework.....	7
Operational Definitions.....	8
Assumptions, Limitations, and Delimitations.....	9
Assumptions.....	9
Limitations	9
Delimitations.....	10
Significance of the Study	10
Impact Value to Business.....	10
Contribution to Effective Practice of Business.....	12
Implications for Social Change.....	13
A Review of the Professional and Academic Literature.....	13
Conceptual Framework.....	15

Overview.....	19
Threat Methodologies	23
Attack Methodologies.....	25
Defense Methodologies	27
Cyber Security Strategies.....	32
Emerging Technologies	35
Transition	49
Section 2: The Project.....	51
Purpose Statement.....	51
Role of the Researcher	52
Participants.....	55
Research Method and Design	59
Research Method	60
Research Design.....	62
Population and Sampling	64
Ethical Research.....	69
Consenting Process	69
Participant Withdrawal Process	70
Measures for Ethical Protection.....	71
Data Retention Protection Plan.....	71
Data Collection Instruments	72
Data Collection Technique	75

Data Organization Technique	78
Data Analysis	80
Codes Developed for Interview	85
Development of Coding System	85
Interview Coding Summary	86
Data Analysis Summary and Presentation	87
Reliability and Validity	87
Reliability	87
Validity	89
Transition and Summary	92
Section 3: Application to Professional Practice and Implications for Change	95
Introduction	95
Presentation of the Findings	95
Theme 1: Cyber Security Strategy	98
Theme 2: Reliance on Third-Party Vendors	109
Theme 3: Cyber Security Awareness	114
Applications to Professional Practice	120
Implications for Social Change	122
Recommendations for Action	123
Recommendations for Further Research	125
Reflections	126
Conclusion	128

References	129
Appendix A: SME Owner’s Cyber Security Strategies Interview Questions.....	165
Appendix B: Participant Recruitment Letter	166
Appendix C: Interview Protocol	167
Appendix D: Study Participant Thank-You Note	169
Appendix E: Study Participant Member Checking.....	170
Appendix F: Study Participant Comments of Data Interpretation File.....	171
Appendix G: Study Participant Interpretative Responses File	172

List of Tables

Table 1. Sample Coding List for Reflective Journal and Research Log.....	79
Table 2. Coding Legend.....	86
Table 3. Cyber Security Measures to Limit Access.....	101

List of Figures

Figure 1. Emergent themes of SME owners' effective cyber security strategies	96
Figure 2. SME owners' cyber security prevention subthemes	99
Figure 3. SME owners' successful cyber security strategy subthemes	100
Figure 4. SME owners' preferred employee training methods.....	108
Figure 5. SME owners' reliance on third-party vendor subthemes	110
Figure 6. SME owners' cyber security awareness subthemes	115

Section 1: Foundation of the Study

The way people share knowledge, conduct electronic business, and create value was revolutionized by the Internet, which is becoming increasingly important for conducting business (Askitas & Zimmermann, 2015; Jansen, Veenstra, Zuurveen, & Stol, 2016). In the 21st century, small business owners use computer systems and the Internet to compete in the technology-infused global e-commerce markets (United States Small Business Administration [SBA], 2016a). Improvements in global wired and wireless technology provide businesses enormous benefits, yet simultaneously expose companies to potential vulnerabilities (Weber & Horn, 2017). In 2014, victims of cyber incidents reported an estimated annual loss due to cyber crime at \$400 billion a year (Arief, Bin Adzmi, & Gross, 2015).

Small and medium-sized enterprise (SME) owners often lack the necessary information technology resources and capabilities needed to implement emerging cyber security recommendations (Harris & Patten, 2014). Specifically, SME owners regularly lack the proper processes to control evolving cybersecurity risks and information systems security threats that characterize the use of these technologies (Njenga & Jordaan, 2016). Theft or loss of private information can be an expensive casualty to any business (Piggin, 2016); however, for SME owners, negative losses resulting from cyber attacks might be unrecoverable (SBA, 2015). The loss of customers, income, and in some instances forfeiture of business due to expensive litigation costs are among the potential adverse effects on SME owners (Federal Communications Commission [FCC], 2014; Layton & Watters, 2014). Managing cyber risks requires organizations to implement multi-tiered

security strategies focused on prevention, mitigation, and reaction while concentrating on people, processes, and systems (National Institute of Standards and Technology [NIST], 2015a, 2015b). The purpose of the study was to explore effective strategies small business owners used to protect their businesses from cyber attacks.

Background of the Problem

Daily over 2.3 billion people use online technologies to work, learn, bank, shop, and date (Central Intelligence Agency [CIA], 2015). Cyber criminals want access to computers, tablets, and phones because they contain valuable exploitable information, and they are always devising new ways to attack networked technologies (Symantec Corporation, 2015). Cyber criminals use mobile phones, tablets, laptops, and server computers to commit crimes (FCC, 2014).

In 2014, cyber attackers were responsible for 49% of data breach attacks, and SMEs were the primary targets of cyber attacks (Symantec Corporation, 2015). In 2015, cyber attacks against SMEs continued to increase; however, many of these attacks were directed to fewer organizations (Symantec Corporation, 2016). Business owners must be aware of and proactive in implementing new security strategies to protect their corporate and personal client data. New and innovative hardware and software technologies are essential to ensuring business systems and critical infrastructure are resilient (Maughan, Balenson, Lindqvist, & Tudor, 2015).

Giboney, Proudfoot, Goel, and Valacich (2016) described how security hackers pose a continuous and unrelenting threat to organizations by exploiting their computer systems. Moreover, the FCC (2014) emphasized the importance of effective cyber

security practices as a critical factor to ensure Internet communications remain protected, and that individuals of every organization should have security awareness. According to E. B. Kim (2013), cyber crimes are diversified and broad reaching. Owners' cyber security awareness and proactive actions can potentially limit future cyber crimes and increase small business cyber survivability.

Problem Statement

Cyber attacks are increasing, and victimization of individuals, businesses, and governments will regularly continue to occur (Desai, 2013; Federal Bureau of Investigation [FBI], 2015a; Walker-Osborn & McLeod, 2015). In 2013, estimated cyber crime losses exceeded \$67.2 billion annually for U.S. companies (Filshtinskiy, 2013). In 2014, 60% of all targeted cyber attacks struck SMEs whose owners were disadvantaged in protecting their infrastructures (Symantec Corporation, 2015; United States Securities and Exchange Commission [SEC], 2015). SME owners often do not view themselves as targets for cyber attacks due to their small size or the perception they have nothing worth stealing (SBA, 2015). The general business problem is 80% of SME owners do not use adequate processes to protect against cyber attacks (Shackelford, Fort, & Prenkert, 2015). The specific business problem is some SME owners may lack effective cyber security strategies to protect their businesses from cyber attacks.

Purpose Statement

The purpose of the qualitative multicase study was to explore effective strategies SME owners used to protect their businesses from cyber attacks. The specific population consisted of four SME owners operating in the Melbourne, Florida area who utilized the

Internet for business operations. Additional study selection criteria required that SME owners (a) were licensed to operate a retail business in Melbourne, Brevard County, Florida; (b) employed between one and 249 personnel; (c) had an annual gross revenue under \$10 million; and (d) had successfully implemented cyber security strategies.

Given the findings reported by the National Cyber Security Alliance (NCSA, 2015) and in the U.S. House of Representatives Committee on Small Business hearing on “protecting small businesses against emerging and complex cyber-attacks” (2013), I determined that the selected population in this study was appropriate because 60% of SMEs go out of business within 6 months after the first cyber attack. Findings from my study may provide SME owners effective strategies to protect against a cyber attack, which may increase consumer confidence and result in greater economic prosperity for the local community. SME owners who have survived cyber attacks might spur economic growth by employing community residents, fueling the socioeconomic lifecycle.

Nature of the Study

I chose qualitative research methodology for the research study. Researchers use qualitative methods to explore contemporary, real life situations, understand a phenomenon, identify events’ significance, answer questions, and capture descriptions of human experiences (Baškarada, 2014; Houghton, Murphy, Shaw, & Casey, 2015; Yin, 2014). I determined that the qualitative method was most appropriate for this study because my intent was to explore effective strategies SME owners have implemented to deter cyber breaches. Quantitative researchers test hypotheses and describe, categorize,

or relate comparison groups to provide trend analysis on attitudes and opinions to explain and provide understanding of the social phenomena (Palinkas, 2014; Yilmaz, 2013; Yin, 2014). Likewise, mixed methods research combines both qualitative and quantitative methodologies (Azhar, Latif, Murtaza, Khan, & Hussain, 2013; Mayoh & Onwuegbuzie, 2015; Tong, Chapman, Israni, Gordon, & Craig, 2013). To explore effective cyber security strategies, I did not test hypotheses, which are part of a quantitative analysis or the quantitative portion of mixed methods study.

I chose a multicase study design for the study because it is the preferred strategy when asking *how* and *what* questions. According to Hyett, Kenny, and Dickson-Swift (2014), the case study approach is especially appropriate for qualitative research questions, which require a detailed understanding of social or organizational processes. Researchers use case study design to explore a bounded system over time through detailed in-depth data collection, using multiple data sources in a rich, real life framework (Baškarada, 2014; Boblin, Ireland, Kirkpatrick, & Robertson, 2013; Marshall, Cardon, Poddar, & Fontenot, 2013; Yin, 2013).

A multicase study is the most suitable choice to explore the research question using archival data and participant interviews. The ethnographical research design requires researchers to observe participants in their natural habitats to gain a deeper understanding of how people experience, perceive, create, and navigate the social world (Hallett & Barber, 2014; Murthy, 2013; Perry, 2013). Ethnographic design was not appropriate for this study given that my goal was not to understand the cultural practices of a specific group. Researchers use phenomenological design to examine the meaning

of lived experiences of an individual or group of people related to a unique phenomenon (Gale, Heath, Cameron, Rashid, & Redwood, 2013; Mayoh & Onwuegbuzie, 2015; Tuohy, Cooney, Dowling, Murphy, & Sixsmith, 2013). The phenomenological design was not appropriate because I did not explore lived experiences in this study.

Research Question

The following research question guided the study: What effective strategies do SME owners use to protect their businesses from cyber attacks?

Interview Questions

I conducted semistructured interviews focused on investigating effective cyber security strategies SME owners used to protect their businesses from cyber attacks. The following were the eight interview questions I asked each participant:

1. What successful strategies do you use to protect your infrastructure from cyber attacks?
2. What successful strategies do you use for preventing, detecting, and responding to cyber attack incidents?
3. How do you assess your information technology security risks?
4. What employee training strategies do you use for security procedures with Internet devices?
5. What risk management strategies do you use to identify and evaluate cyber attack risks?
6. What is your cyber attack contingency plan?

7. What effective strategies would you recommend to other SME owners to prevent a cyber attack?
8. What additional information on cyber security strategies would you like to provide or expound upon before ending the interview?

Conceptual Framework

I selected the general systems theory (GST) as the conceptual framework for the study. Von Bertalanffy (1968) developed systems theory, which he characterized as the study of interrelationships rather than individual modules. Von Bertalanffy contended that systems, in essence, are self-regulating and self-correcting. Kuhn (1970) extended von Bertalanffy's works by proposing scientific advancement is not evolutionary, but a systematic process where knowledge increases to the limits of the current paradigm, and through scientific revolutions, one worldview replaces another resulting in a paradigm shift. Leaders who apply the system thinking principle are more adept at working within organizational structures, and are better able to manage processes and people within broader environments (Black & Copsey, 2014). Moreover, Young and Leveson (2014) suggested that the GST approach provides a robust foundation for security.

Gomes (2015) noted that SMEs are systems consisting of different components, one of which is information security. As cyber attacks increase, cyber security for SME owners is a critical systems component (Atoum & Otoom, 2016). Cyber security technologies are inadequate to achieve secure operations without strategies, procedures, ongoing risk assessment, and review of secure network protocols to achieve efficient and secure information delivery (Dunn Cavelty, 2014; Wang & Lu, 2013). Applying von

Bertalanffy's GST approach to SME owners' cyber security strategies may capture the influences under which they operate in an unpredictable, dynamically changing cyber-dependent market (Pouvreau, 2014). Exploring successful strategies SME owners have implemented to protect their businesses from cyber attacks may contribute to SME owners' best practices, increase consumer confidence, and result in greater economic prosperity.

Operational Definitions

Cyber crime: The criminal or harmful acquisition and manipulation of data for gain using networked computers to assist perpetration of a crime, such as terrorism, espionage, computer misuse, and fraud, across local or international networks (FBI, 2014; Kraemer-Mbula, Tang, & Rush, 2013).

Evil hacker: An evil hacker is a person whose computer expertise results in malicious intent to sabotage or obtain revenge (Sigholm, 2013; Xu, Hu, & Zhang, 2013).

Insider threats: Insider threats are malicious threats to an organization coming from people inside the organization such as employees, business associates, subcontractors, and even former employees who have intentionally misused their access to negatively affect the confidentiality, integrity, or availability of the firm's information or information systems (Chou, 2013; Internet Crime Complaint Center [IC3], 2014).

Outsider threats: Outsider threats are malicious threats to individuals, organizations, and governments from evil hackers, nonstate sponsored groups, terrorist groups, and members of organized crime (FBI, 2015a; Zhang, Tsang, Yue, & Chau, 2015).

SME: A SME is a business independently owned and operated, which is not dominant in its field of operation (SBA, 2015). The SBA defines different size standards for each industry that relate to the dollar size of the business or the number of employees it has, adjusted for industry (SBA, 2016b; U.S. Census Bureau, 2013).

Assumptions, Limitations, and Delimitations

Assumptions

Jansson (2013) noted that research assumptions are ideas the researcher accepted as true. In this doctoral study, I made four assumptions. The first assumption was that the review of company documents and semistructured interviews would provide sufficient data to answer the overarching research question, and would be sufficient for triangulation. The second assumption was that I would be able to reduce or eliminate the effect of personal bias. The third assumption was that I would be able to conduct effective interviews and solicit authentic responses from the participants. The fourth assumption was that the participants would understand the questions and provide honest answers.

Limitations

Research limitations are constraints over which the researcher has no control and limit the possibility of transferability of the research findings to other situations (Yilmaz, 2013). The first limitation of the study was the selected participants understand the interview questions and provide honest answers. The second limitation was the availability of selected participants for personal interviews to support timely data collection. The third limitation was the review of company documents and

semistructured interviews would provide sufficient data to answer the overarching research question and suffice for triangulation purposes.

Delimitations

Research delimitations enable researchers to limit the scope and variables of their research study (García, Skotnicka, & Zamora, 2015; Marshall & Rossman, 2016).

Research quality is dependent upon the investigator's ability to deflect personal biases and present research data in an objective manner (Smith & Noble, 2014). I delimited the study to SME owners who (a) were licensed to operate a retail business in Melbourne, Brevard County, Florida; (b) employed between one and 249 personnel; (c) had an annual gross revenue under \$10 million; and (d) had successfully implemented cyber security strategies. Exclusionary delimitations included SME owners who did not meet all of the criteria.

Significance of the Study

Impact Value to Business

My findings on SME owners' effective cyber security strategies may be valuable to individual consumers, other SME owners, third-party software vendors, cyber hackers, coders, and academics, as well as municipal, state, and federal government agencies. Case study research on cyber security phenomena may provide valuable information enabling SME owners to avoid becoming victims of cyber security breaches. Not only do cyber security breaches have the potential to impact SME owners financially, but they also create additional management problems such as employees' frustrations as they deal

with possible adverse customer feedback, systems downtime, and loss of productivity (Hayes & Bodhani, 2013; Hua & Bapna, 2013).

Alternatively, Gordon, Loeb, and Zhou (2016) reported cyber security investments could give organizations a competitive advantage by generating additional benefits, such as increased revenues. The majority of malicious computer security attacks are preventable by utilizing various security protection methods, thus disabling installation of viruses, malware, and spyware on host computers and mobile devices (Egele, Scholte, Kirda, & Kruegel, 2012; FCC, 2014; Tchakounté, 2014). Business owners, regardless of the size of their enterprises, are potential cyber crime victims and should invest in securing their data (FCC, 2014; SBA, 2015). Effective strategies for protecting data require business owners to be aware and proactive, and to implement effective security measures to defend against cyber threats (Gupta, Seetharaman, & Raj, 2013).

There are computer users whose sole purpose is to exploit the weakness in a system for self-profit or gratification (Chowdappa, Lakshmi, & Kumar, 2014). Ethical and malicious computer hackers are patient and diligent in discovering ways to enter and infiltrate infrastructure weaknesses; only the intention of the hackers makes them diverse (Chowdappa et al, 2014). Computer users should take precautions when using a network device (FCC, 2014).

Securing cyber space is one of the nation's top priorities. However, it is not only a national effort, but also a global effort (The White House, 2014). Companies must invest in preventative technologies to provide an initial layer of protection between

themselves and cyber hackers. Technologists have suggested corporations, consumers, and government entities must invest in innovative solutions, which are years ahead of any criminal hacking concept to protect global wired environments (Livshits, Bace, & Neville-Neil, 2013).

Contribution to Effective Practice of Business

Cyber attacks are rapidly increasing, and economic impacts are beginning to affect the global economy (Kshetri, 2013). Cyber security strategies cannot prevent personnel authorized to access information from sharing it with those who are not (Bambauer, 2013). SME owners must develop effective cyber security countermeasures to protect their companies' transactions (FCC, 2014; Fielder, Panaousis, Malacaria, Hankin, & Smeraldi, 2016; SBA, 2015).

According to the FBI's IC3 (2014), Florida was ranked number two in cyber victim complainants. Cyber crime appears to be growing at a rapid pace with ever-changing, emerging technologies and dependence on the Internet (Rashid & Parvez, 2014). In this study, I have identified factors that may improve SME owners' awareness of cyber security strategies and preventative actions. Implementing successful strategies promotes positive economic and social benefits, which increase local consumer confidence while minimizing consumer risks (FBI, 2015a). Additionally, the results of the study may be useful to SME owners who frequently use Internet-connected devices and may not focus resources on implementing affordable and sustainable cyber security strategies.

Implications for Social Change

One of the biggest issues facing SME owners is the ability to defend themselves from potential cyber attacks (Fielder et al., 2016). At present, SME owners have limited strategies to address cyber security vulnerabilities and implement effective preventative measures. Positive social change resulting from this study includes the potential for SME owners to utilize cyber security best practices to alleviate or mitigate future cyber attacks.

Findings from the study may provide SME owners with effective strategies to protect against a cyber attack, which may increase consumer confidence resulting in greater economic prosperity. The implications for positive social change include empowering other SME owners and new entrepreneurs with strategies and resources to effect changes within the community. The findings in this study may transform the way SME owners view cyber security strategies, and help SME owners who survive cyber attacks spur economic growth by employing residents of the community, thereby stimulating the socioeconomic lifecycle.

A Review of the Professional and Academic Literature

The purpose of this qualitative multiple case study was to explore what effective strategies SME owners used to protect their businesses from cyber attacks. The Internet has played a significant role in transforming modern life and requiring users to keep their data secure from unauthorized distribution (Kortjan & Von Solms, 2014; Kumar & Chaudhary, 2014). The targeted population consisted of SME owners who operated retail businesses located in Melbourne, Florida, used the Internet for business operations, and had successful cyber security strategies.

In a recent study, researchers estimated that the economic losses due to cyber attacks will exceed \$20 trillion by 2020 (Srinidhi, Yan, & Tayi, 2015). SME owners are disadvantaged in protecting their infrastructures against cyber attacks (SEC, 2015), and many SME owners conduct business over the Internet without using any security features (SBA, 2014). Eighty percent of small business owners do not have established cyber security policies (Shackelford et al., 2015).

The purpose of my academic literature review was to compare and contrast different and opposing views related to the research topic. My search efforts were focused on electronic information I obtained through published dissertations, government websites, and peer reviewed journals available through the Walden University Library, Google Scholar, and web pages. Hyperlink results provided access to scholarly information from EBSCOhost, ProQuest, Business Source Complete, IEEE Source Library, government websites, and other multidisciplinary research databases.

The search criteria included the following keywords: *browser security, business failures, cloud computing, computer crimes, cyber attacks, cyber bullying, cyber crimes, cyber fraud, cyber hacking, cyber loss, cyber security, cyber war, data loss, data theft, e-mail phishing, espionage, ethical hacking, fraud, hackers, hacking, network loss, network prevention, security, security detection, security prevention, small business, and software theft*. I used the Ulrichsweb global serials directory database engine to validate the peer reviewed and scholarly reference listings. Additionally, if an entry was not listed in Ulrichsweb search engine results, I used the journals' homepages to validate the peer reviewed and scholarly reference listings.

The literature review consisted of 137 references, of which 121 sources (88%) were peer reviewed and published between the years 2013 and 2017. Twelve sources (9%) were peer reviewed but not published between the years 2013 and 2017, and four sources (3%) were published between the years 2013 and 2017 but were not peer reviewed. Included in my review were one dissertation, two scholarly magazines, two seminal books, four industry websites, 25 government websites, and 103 journal articles.

Prior studies have indicated that cyber attacks are on the rise, and that potential adverse financial impacts are devastating (Desai, 2013; FBI, 2015a; Kongnso, 2015; Walker-Osborn & McLeod, 2015). This literature review consists of the opening narrative and discussions of its application to the business problem and conceptual framework. It is then thematically divided into six major subsections: overview, threats, attack methodologies, defense methodologies, cyber security, and emerging technologies.

Conceptual Framework

Von Bertalanffy (1968) developed systems theory, which he characterized as the study of interrelationships rather than individual modules. Von Bertalanffy contended that systems, in essence, are self-regulating and self-correcting. Kuhn (1970) extended von Bertalanffy's works by proposing scientific advancement is not evolutionary, but a systematic process where knowledge increases to the limits of the current paradigm, and through scientific revolutions, one worldview replaces another resulting in a paradigm shift. Caws (2015) described von Bertalanffy's GST as a theory of open systems which can be opened in various ways and closed by the selective admission of nearby elements. Leaders who apply the system thinking principle are more adept at working within organizational

structures, and better able to manage processes and people within broader environments (Black & Copsey, 2014).

Bambauer (2013) described the current theoretical approaches to cyber security as significantly flawed, and noted that scholars, governments, and computer scientists agree inadequate security is an emerging threat and preventative action is urgently required. The cyber security problem includes economic and structural factors requiring increased regulation; the reality is cyber threats are inevitable (Bambauer, 2013; Dunn Cavelty, 2013). Gomes (2015) stated that SMEs are systems consisting of different components, one of which is information security. As cyber attacks increase, cyber security for SME owners is a critical systems component (Atoum & Otoom, 2016). Cyber security technologies are inadequate to achieve secure operations without strategies, procedures, ongoing risk assessment, and review of secure network protocols to achieve efficient and secure information delivery (Dunn Cavelty, 2014; Wang & Lu, 2013).

Young and Leveson (2014) suggested that the GST approach provides a robust foundation for security. Applying von Bertalanffy's GST approach to SME owners' cyber security strategies may capture the influences under which they operate in an unpredictable, dynamically changing cyber-dependent market (Pouvreau, 2014). Exploring successful strategies SME owners have implemented to protect their businesses from cyber attacks may contribute to SME owners' best practices, increase consumer confidence, and result in greater economic prosperity.

The objective of the study was to explore what effective cyber security strategies SME owners used to protect their businesses from cyber attacks. Pervasive and sustained

cyber attacks could have a potentially devastating impact and could disrupt the operations of individuals, businesses, and governments (United States Government Accountability Office [GAO], 2013, 2015). On February 12, 2013, President Obama issued Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, directing the NIST to work with over 3,000 government, industry, and academia stakeholders to develop a voluntary framework based on existing standards, guidelines, and practices to reduce cyber risks to critical infrastructure (NIST, 2015b; The White House, 2015a).

The *Framework for Improving Critical Infrastructure Cybersecurity Version 1.0*, published on February 12, 2014, provides a list of activities to achieve specific cyber security outcomes (NIST, 2015a). The framework provides elements to identify and prioritize actions for reducing cyber security risk and can help businesses align policy and technological methodologies to manage those risks (NIST, 2015a). The NIST organization focuses on awareness, cyber security education, training, and professional development (NIST, 2015a; Paulsen, McDuffie, Newhouse, & Toth, 2012).

Typically, large businesses have entire IT organizations dedicated to addressing advanced persistent attacks and updating security policies, whereas small businesses normally do not have the same resources to deter cyber attacks. IT experts have argued that the cyber security framework represents the best efforts to address a threat, which President Obama has called one of the gravest national security dangers the United States faces (Shackelford et al., 2015). The NIST cyber security framework is a global plan of action to guide users by using best practices to develop policies, training, and control

plans to improve or maintain their cyber security (NIST, 2015a; United States Department of Homeland Security [DHS], 2015c).

The NIST framework includes standards, guidelines, and practices for SME owners, highlighting the basics of cyber security and information security, defining the type of information needing protection, discussing common cyber threats, and informing users of known cyber security best practices (NIST, 2015b; Schneck, 2014). The NIST (2015b) cyber security framework provides SME owners the best overall framework and guidelines for protecting information, and it provides the primary tenants for computer and network security strategies. The NIST framework began in 2010 as part of an effort under the National Initiative for Cybersecurity Education (NICE) to expand the Comprehensive National Cybersecurity Initiative from an internal federal activity to an external national activity (Paulsen et al., 2012).

Moreover, the government created NICE with the idea that the most important element in the fight against cyber threats is people. People create the technologies that protect information and resources, they recognize cyber threats and respond to them, and they understand how to protect themselves and others in cyber space (Paulsen et al., 2012). The NIST agency's primary focus is to promote awareness, formal education, training, development, and workforce structure. Additionally, this new private public partnership emphasizes collaboration with other government agencies, industry, communities, and academia for individuals and groups to improve the cyber behavior, skills, and knowledge of worldwide technology users (Paulsen et al., 2012). The NIST

voluntary cyber security framework is destined to become the next national benchmark for assessing an organization's cyber security (NIST, 2015a).

Technological advancements have made critical infrastructures more vulnerable (Jaradat & Keating, 2014). Bambauer (2013) explained that computer and network security problems exist because cyber security is undertheorized and lacks a framework to guide change. Likewise, Jaradat and Keating (2014) examined critical infrastructures from a systems view, and suggested that interdependences between critical infrastructures are becoming increasingly apparent and that understanding how to manage critical infrastructures is an emerging issue for businesses. Global interconnections have caused systems to converge, meaning an isolated attack on one critical infrastructure system can result in a cascading effect on other critical infrastructures and affect business operations (Jaradat & Keating, 2014). Exploring effective SME owners' strategies aligns with the systems theory conceptual framework.

Overview

Cyber attacks are actions by individuals or groups of people attempting to bypass security mechanisms of computer and network systems (FBI, 2016; Raiyn, 2014). Cyber crime is a relatively new phenomenon with potentially severe consequences for local and global businesses if not adequately addressed. Intellectual property, patents, and critical business information are valuable assets (FCC, 2014). The SBA (2012) reported SMEs produced 16 times more patents per employee than large patenting firms. SMEs are an important part of the nation's economy, but their owners often do not view themselves as targets for cyber attack (SBA, 2015).

Symantec Corporation (2015, 2016) conducted studies of SMEs to determine their susceptibility to cyber attacks; results indicated SMEs are susceptible to cyber attacks because they lack sophisticated security capabilities and the financial resources to prevent potential attacks. Cyber attacks on SMEs may enable access to system backdoors, exponentially expanding potential losses (MacEwan, 2013). My objective in this qualitative research study was to explore successful strategic elements of cyber security and the prevention methodologies employed by SME owners to protect their businesses from cyber attacks. Cyber criminals are increasing attacks on small business owners who currently may have limited information on cyber security vulnerabilities and protective strategies (SBA, 2014).

Trends in the literature indicate cyber attacks are vast and cover many facets of Internet connectivity (Jang-Jaccard & Nepal, 2014). The term *cyber attack* includes three primary areas of criminal activity: cyber terrorism, cyber identity theft, and cyber espionage (FBI, 2013a). Cyber terrorists are state-sponsored and non-state actors who engage in computer and network intrusions to pursue cyber space attacks and cause public fear (Sigholm, 2013). Cyber identity theft occurs when someone unlawfully obtains another's personal information and uses it to commit theft or fraud (FBI, 2016). Cyber espionage is politically motivated hacking focused on national security breaches and sabotage of a nation's critical infrastructure (Jang-Jaccard & Nepal, 2014). While each area contains specific technological advances and methods to perform tasks, the two commonalities each share are access to connectivity and user vulnerabilities. After conducting extensive research about cyber security, I found that the United States is not

alone in its efforts to combat cyber attacks and mitigate cyber crimes (Embassy of the United States, 2013; The White House, 2014).

Technology is a valuable commodity to people, businesses, and governments. In October 1957 when Russia successfully launched Sputnik 1, the first space satellite (Kuznetsov, Sinelnikov, & Alpert, 2015), the U.S. government was caught off guard. To regain their premier and most advanced superpower status, the U.S. Department of Defense (DoD) awarded multiple contracts to the Advanced Research Project Agency (ARPA), now known as the Defense Advanced Research Project Agency (DARPA) (Campbell-Kelly & Garcia-Swartz, 2013). One such contract involved American scientists who theorized developing a network of dispersed nodes for educators to communicate with each other over internetworking paradigms using specific communication protocols. In 1969, Cerf and Kahn's theory was tested and proved successful with the first electronic message transmission between two computers: from the University of California Los Angeles (UCLA) to the Stanford Research Institute (Campbell-Kelly & Garcia-Swartz, 2013).

Eventually, network and computer developers connected additional computers to the educational network, exponentially expanding it to the global Internet of today, a system of diverse networks connected through standard communication protocols (Campbell-Kelly & Garcia-Swartz, 2013). Campbell-Kelly and Garcia-Swartz found the developers of the first Internet protocols (IP) did not consider security issues thus fueling the prominence of current cyber security attacks. Haigh (2014) accurately reported one person did not develop the Internet, which has evolved over time. The Internet has

transformed the entire global society by enabling information sharing and spurring economic growth and prosperity.

Cyber espionage of American companies in 2009 exceeded \$50 billion while global losses from cyber hacking surpassed \$1 trillion (Ezekiel, 2013). The U.S. government designed the EINSTEIN program as the first line of defense on national security prevention against cyber attacks (Malik, 2013). The basis of EINSTEIN's first cyber attack strategy was to limit network access points and prescreen incoming network traffic from malicious attacks. In 2002, the U.S. government established the DHS with its primary focus to protect the U.S. and its territories from accidents, terrorist attacks, and natural disasters (DHS, 2015b). Additionally, the DHS has responsibility for protecting critical national infrastructures, which include the Internet (DHS, 2015b). The DHS faces many Internet security challenges in its efforts to prevent millions of daily cyber attacks (DHS, 2015a).

While large organizations have the methods to determine such losses, SME owners often, lack the capability and ignore the implementation of effective network security measures, which result in high risk exposure and losses from cyber attacks (SBA, 2014). SME owners prioritize their cyber security strategies by understanding their risk tolerance to mitigate potential cyber attacks (Fielder et al., 2016). Those who ignore or fail to implement security measures risk exposure to becoming cyber attack victims (DHS, 2015a).

Threat Methodologies

Prior studies have indicated cyber attacks are on the rise and that becoming a cyber attack victim will be a normal occurrence without modifications to national security and enforcement policies (Desai, 2013; FBI, 2015a; Kongnso, 2015; Walker-Osborn & McLeod, 2015). Likewise, Filshtinskiy (2013) reported the estimated losses for domestic U.S. companies affected by cyber crime exceeds \$67.2 billion annually. Although cyber criminals continue to find creative ways to penetrate laptops, phones, and computer networks resulting in numerous cyber security attacks and thefts, the key to effective cyber security is managing organizational risks (Sheppard, Crannell, & Moulton, 2013). Hacking evolved over time spawning into transgressive criminal expertise (Steinmetz, 2014). State and non-state hackers perform cyber operations to achieve a mixture of political, economic, or military objectives (DoD, 2015). Hackers comprise three groups: (a) a *black hat* or evil hacker with malicious intent to sabotage or obtain revenge; (b) a *white hat* or ethical hacker, usually a security professional or a penetration tester; and (c) a *grey hat* or a person who hacks for curiosity and notoriety and, in some cases, is a former black hat now employed as a security professional (Sigholm, 2013; Xu et al., 2013).

Evil hackers are responsible for some of the recent cyber attacks on Coca-Cola, Target, and the Office of Personnel Management (OPM) (Arlitsch & Edelman, 2014; Gootman, 2016). Cyberspace is an unpredictable environment characterized by non-linear dynamics in which effects are disproportionate to their apparent causes (Betz &

Stevens, 2013). The FBI reported global organized crime activities as one of the most sophisticated reaping illegal profits exceeding \$1 trillion per year (FBI, 2015b).

Cyber threats are increasingly affecting businesses' bottom lines; however, business owners are often dismissing warnings. Few businesses are taking the necessary steps to safeguard their private data and enhance cyber security (Shackelford et al., 2015). The implications and threats posed by security breaches have the potential to crush even the most intimate aspects of lives (Desai, 2013). There are two categories of threats: insider and outsider (FBI, 2015a; Zhang et al., 2015).

To mitigate insider attacks, Mandal and Chatterjee (2015) proposed controlling the system administrator's activities and proposed policy changes for system administrators. Hua and Bapna (2013) reported simulation results indicate the optimal investment required to protect an information systems infrastructure from insiders is several magnitudes higher than for protecting against external hackers. Effective security countermeasures are dependent on understanding the user's behavior and his or her susceptibility to hackers and scam artists (Zhang et al., 2015).

In many firms, the business value for information technology (IT) is a top concern. Chen et al. (2014) reported the positive effects of IT capability on organizational performance but cited our knowledge of the processes through which such gains are achieved remains limited due to a lack of focus on the business environment. Kongso (2015) conducted a qualitative study of 14 participants consisting of four technology executives and 10 technology staff to determine the best practices technology leaders use to minimize data security breaches yielding increased business performance.

Research study findings revealed executive business leaders lacked sufficient knowledge to minimize data security breaches for increased business performance (Kongnso, 2015).

Attack Methodologies

Instigators of both outsider and insider threats use attack methodologies to alter or destroy data or functionality of networks or systems (FBI, 2015a). One example is the hacker's use of bogus security certificates or certificates of authority (CA) which enable Internet users to operate using secure transmissions (Laurie & Doctorow, 2012). Hackers then have unlimited access to the Internet via the compromised computers because the bogus certificates appear to be authentic. In an effort to fix the problem, Laurie and Doctorow (2012) proposed using a cryptographic protocol called sovereign keys (SK), which includes additional verification features, as a new security mechanism for vendors to implement. Internet system administrators continue to explore and deploy solutions to identify and eliminate the use of bogus security certificates.

Gordon et al. (2016) reported cyber security investments could give organizations a competitive advantage generating additional benefits, such as increased revenues. SME owners should develop cyber security strategies focusing on confronting human vulnerabilities (Zhang et al., 2015). Researchers indicated users are aware of proper password management, yet are still inclined to take risks (Whitty, Doodson, Creese, & Hodges, 2015).

The explosion of online and mobile technologies has resulted in a timeless global workplace. Engineers design computer and network systems to operate with services, security mechanisms, and attacks running simultaneously without affecting overall

system performance (Emm, 2013). Denial of service attacks, spyware, and viruses are examples of components affecting computer and network performance (Emm, 2013; Ye, Aranda, & Hurley, 2013).

The growth of the mobile market has sparked a revolution of employees who bring their smart phones or tablet devices to use at work locations. Although there may be advantages for Bring Your Own Device (BYOD) systems, which reduce a company's indirect costs, one of the biggest risks involves employees downloading personally identifying or confidential client information to their smartphones and/or tablet devices (Disterer & Kleiner, 2013). Thieves could then obtain critical company data if any of those mobile devices were lost, stolen, or otherwise compromised. To mitigate the effects of the attack methodology, SME owners can establish policies for employee use of public Wi-Fi zones, and require employees utilize a virtual private network (VPN) for connectivity when connecting to a corporate network (Disterer & Kleiner, 2013).

SME owners must be knowledgeable of BYOD systems and develop appropriate security strategies to mitigate inadvertent company exposure to cyber attacks (MacEwan, 2013). Moreover, business owners must operate under strict regulations to protect client data (FCC, 2014; SBA, 2014, 2015). The adoption of cloud computing has many benefits enabling SME owners to compete globally in a cost-effective manner with seamless sharing of cloud infrastructure and computing resources. Abdellaoui, Khamlichi, and Chaoui (2016) reported numerous features and advantages; however, the cloud has also brought some issues, particularly, security and monitoring. One of its primary security concerns is the weak user authentication.

The U.S. has classified cyber space attacks as an act of war, which allows the use of military force to combat intrusions (DoD, 2015). Academic computer scientists are in a unique position to influence and shape national and international cyber security policies by determining what type of information is required for cyber attack assessments (NIST, 2015a, 2015b; Shackelford et al., 2015). Although the current global political environment and recommendations by national policy makers are influencing factors, federal, state, and local officials are ultimately responsible for making decisions to defend the nation from cyber attacks (The White House, 2014).

Defense Methodologies

Hu and Scott (2014) argued software security prevents leaks of data, alteration of data, and unauthorized access to data. Determining the level of system vulnerability is essential to identifying and developing an appropriate security infrastructure methodology (NIST, 2015b). The top five operating system characteristics for monitoring system impacts for motion detection, intrusion detection, and cyber attacks are the system, process, memory, network, and IP (Ye et al., 2013). Varied system performance objects, such as task manager, monitor the state and performance of systems, detect attack activities, and trigger appropriate security systems protection (Li, 2013; NIST, 2015b; Ye et al., 2013).

SME owners are more vulnerable to cyber attacks than large enterprises because they may lack the IT expertise and resources needed to understand and confront IT security issues in the rapidly growing threat environments (Emm, 2013). According to a 2016 study conducted by Jansen et al. (2016), SME owners implemented protective

measures when they (a) believe a measure is effective, (b) are capable of using Internet technology, (c) have a positive attitude toward online protection, and (d) are responsible for their own online cyber security. Loss of data affects businesses and has the potential to jeopardize a company's reputation with customers, suppliers, and partners (SBA, 2014).

Society's insatiable desire for knowledge has created a repetitive cycle fueling new technology, computing inventions, and sophisticated cyber attacking (Cheswick, 2013; Jang-Jaccard & Nepal, 2014). Business owners' first line of defense to prevent data loss is to implement effective user passwords (Cheswick, 2013). Likewise, Wen et al. (2014) presented study results indicating appropriate authorization and controls are necessary to prevent individuals' data from malicious use and ensures individual privacy when developing an open platform.

Although Cheswick (2013) and Wen et al. (2014) reported that user passwords are critical to potentially preventing data loss, Whitty et al. (2015) reported individuals continue to engage in risky password practices, such as sharing passwords, using the same password over multiple platforms, and despite numerous public campaigns to the contrary, using passwords easily cracked. Business owners who used a process approach to security effectively implement strategies to detect, protect against, and respond to cyber attacks (Lowe, 2014). Additionally, Emm (2013) addressed six security steps, which SME owners can employ to protect themselves (a) require user passwords for login accounts, (b) select products which provide protection, (c) protect and secure systems data, (d) establish and implement user policies and procedures, (e) properly train

staff to recognize and understand the risks, and (f) expect and prepare for the worst. Business owners should implement security policies not only flexible and easily adaptable to counteract emerging cyber threats but also containing data retrieval and backup plans to prevent complete data loss and enable fast retrieval and recovery (FBI, 2014, 2015c).

Different views for implementing loose and strong password criteria depend on the business model and user/customer base willingness and ease to access desired technology. J. Hong and Reed (2013) reviewed password guidelines of international website retailers such as Amazon, Fidelity Investments, and PayPal, which revealed loose security password policies enabled users to easily login and purchase products without stringent verifications. On the other hand, J. Hong and Reed found creating user accounts and passwords on national government websites was extremely difficult due to strong password criteria requirements. Jang-Jaccard and Nepal (2014) and the FCC (2014) recommended business owners' defense methodologies focus on mitigating risks associated with owning and operating information systems.

Prevention. Developing a system of preventive security measures adds a significant deterrent to protect networks from malicious cyber activity (DHS, 2015b; SBA, 2014). Both public and private organizations require a robust cyber security strategic approach to prepare, respond, and recover from cyber attacks (Sheppard et al., 2013). Grossman (2013) analyzed the design of Internet security measures and reported popular Internet browsers do not offer users sufficient security protection and are still susceptible to malware downloads, which was similar to findings in previous studies. To

keep information and data safe, developers must make significant improvements to Internet browsers' security, such as improved multifactor security authentication methods and CAs (Grossman, 2013; Laurie & Doctorow, 2012).

SME owners must be more aware of cyber security if they are going to avoid becoming cyber victim casualties (Hayes & Bodhani, 2013). According to the SBA (2014), SME owners in the U.S. have a false sense of protection from cyber crime attacks. SME owners must take a proactive approach to protecting their data by establishing cyber security plans, and creating and implementing Internet security policies (DHS, 2015b; SBA, 2014). Building secure software involves several different processes, but security awareness and implementation are the most important (Hu & Scott, 2014).

Some businesses are opting to outsource their information security protection services to a third-party managed security service provider (MSSP), which enable SME owners to forgo owning, maintaining, and updating their software and hardware infrastructures (Sultan, 2014). However, outsourcing is not without risks, such as whether the MSSP's protection will be sufficient if a data breach occurs (Jang-Jaccard & Nepal, 2014). Ultimately, a business owner must evaluate whether the risks of outsourcing security protection services to a third-party are necessary to mitigate company losses (FBI, 2014, 2015c).

The Internet has rapidly grown from its inception requiring fundamental legislative changes to keep up with rapidly developing consumer requirements (Kutty & Sreeramareddy, 2014). There are concerns from privacy advocates who fear legislation

will allow unauthorized disclosure of personal information to the federal government (Taddeo, 2013). Both the Federal Trade Commission [FTC] (2016) and Taddeo (2013) reported the need to reach an ethical solution to fine-tune cyber security measures and individual rights. Taddeo reported public authorities' attempts at legislation have resulted in disagreement over cyber security measures and an individual's rights, attributing to the struggle between liberties and authorities.

Garfinkel (2012) expressed concern over cyber security and computer related risks since no single solution addresses the problem of computer security breaches. Rid and Buchanan (2015) reported attribution for computer network intrusions is one of the most intractable technical problems and is dependent on the available forensic evidence. Both Desai (2013) and the White House (2015a) reported on the need to develop cyber space policies and adopt national and international enforcement for social and business transactions including data location, accountability, cyber bullying, crimes, terrorism, and fraudulent activities. Business owners should concentrate their efforts to reduce risks by implementing technical and political solutions (NIST, 2015b; SBA, 2015, 2016b). While awaiting additional cyber space policies and enforcement at the national level, it is imperative for business owners to develop and implement cyber security strategies and preventative measures to mitigate data losses (FBI, 2015a).

Cloud computing. Cloud computing is a time-sharing, on-demand network model, which enables access to a shared pool of configurable computing devices where businesses store and retrieve their data securely at a remote (cloud) location (Whaiduzzaman, Sookhak, Gani, & Buyya, 2014). Users can quickly provision clouds

fully scalable depending on business requirements. Whaiduzzaman et al. (2014) and Rashid and Parvez (2014) agreed the emerging technology fills the void for SME owners whose workforces have immediate access to the Internet by allowing users to access end systems using infrastructure and software provided by the cloud at minimal cost.

Not only does cloud computing relieve SME owners of the indirect information technology burden large businesses have by leveraging virtual data storage and retrieval, it also mitigates huge overhead or indirect costs (Rashid & Parvez, 2014). Cloud computing efficiencies increase profits by allowing more employees to work from remote locations thereby increasing overall company productivity. Additionally, Whaiduzzaman et al. (2014) reported vehicular cloud computing as hybrid technology influencing traffic management and road safety by instantly allowing users to access vehicular computing resources and the Internet for decision-making.

Cyber Security Strategies

The global economy depends on effective cyber security strategies to ensure individual, business, and global governments' infrastructure assets remain secure (FBI, 2015a; The White House, 2015b). Von Solms and Van Niekerk (2013) defined cyber security as the ability to protect or defend cyber space from cyber attacks and includes capabilities allowing detection, assessment, reaction, and exploitation of potential cyber threats in real or near real time. SMEs comprise the majority of businesses in most economies and the potential cyber threats to SMEs could be catastrophic (Yeboah-Boateng, 2013). Defense, exploitation, and attack are three operational domains of cyber security while confidentiality, integrity, and availability are three primary principles of

cyber security (Raza, Wallgren, & Voigt, 2013; Wang & Lu, 2013). President Obama reported cyber security affects the national security, economic prosperity, and personal privacy and is one of the most significant challenges the global economy is unprepared to confront (The White House, 2015b).

Cyber security decisions require insight into current security threats and the ability to forecast potential vulnerabilities (NIST, 2015b). SME owners lack the proper processes to control evolving cybersecurity risks and information systems security threats, which characterize the use of these technologies (Njenga & Jordaan, 2016). According to Verbano and Venturini (2013), because SME owners lack the resources to respond to cyber security threats, which may potentially threaten their survival, they should adopt risk management strategies and methodologies. Cyber security models aid decision-makers by identifying security threats and system vulnerabilities further enabling stakeholders to quantify their risks results in economic terms (Rabai, Jouini, Aissa, & Mili, 2013). Each stakeholder defines specific security requirements and the model adjusts to the identified requirements based on desired security compliance (NIST, 2015b; SBA, 2015, 2016b). Although Rabai et al. (2013) provided a quantitative model for security measurement to quantify risks enabling SME owners to strategize and mitigate losses, Bambauer (2013) recommended a different approach to focus on mitigating breaches rather than preventing them.

Fielder et al. (2016) proclaimed one of the biggest issues facing SME owners is the ability to defend themselves from potential cyber attacks. Kongnso (2015) conducted a qualitative multiple case study exploring best practices technology leaders use to

minimize security breaches and increase business performance. According to Kongso, the four major elements further reducing security breaches and improving business performance are (a) an organizational culture promoting security awareness, (b) consistent organizational security policies and procedures, (c) implementation of security awareness education and training to mitigate insider threats, and (d) organizational commitment to adopt new technologies and innovative processes.

Garfinkel (2012) reported there is evidence that global interconnectedness combined with the proliferation of hacker tools means today's computer systems are less secure than equivalent systems a decade ago. Additionally, Garfinkel stated although IT experts have introduced techniques and technologies to reduce security-critical defects, such as Microsoft's Security Development Lifecycle, they have not been widely adopted. According to Garfinkel, most companies view IT as a cost or product rather than as an enabling technology, with Fortune 500 companies in 2011 spending \$5.3 billion per year on cyber security, stopping just 69% of all attacks. Organizations increased use of mobile devices, cloud services, and Electronic Health Records (EHRs), and exploitation by criminals to commit cyber crimes through handheld devices require organizations to adequately address security and privacy concerns to deter cyber crime activity (Kotz, Fu, Gunter, & Rubin, 2015). As the Internet continues to grow, so does the concern over security threats inflicted by cyber attacks (NIST, 2015a, 2015b). Various researchers, federal organizations, and commercial companies are working together to identify the primary factors, which contribute to a secure business environment (FCC, 2014; NIST, 2015a, 2015b).

Emerging Technologies

SME owners are predominantly disadvantaged in protecting their infrastructures against cyber attacks (SBA, 2014; SEC, 2015). Likewise, Shackelford et al. (2015) reported 80% of owners of small firms do not have established cyber security policies. The damage inflicted by recent cyber attacks demonstrates SME owners should proactively create cyber security strategy plans (SBA, 2014). Strategic planning elements should include how organizations can leverage emerging technologies to assist with their strategic visions and risk assessments (NIST, 2015b).

Developers of home electronic devices deploy cyber technology ranging from the traditional (laptops and desktops) to televisions, toys, appliances, and home automation systems (Denning, Kohno, & Levy, 2013). By leveraging the latest technological inventions, criminals have accessed individuals' home video and audio feeds, unlocked doors, disabled home security systems, tampered with home healthcare devices, and interfered with home appliances and utilities (Denning et al., 2013). Items as insignificant as a bathroom scale are subject to remote data retrieval by unauthorized access (Denning et al., 2013).

Cyber criminals are using society's thirst for technology to plan their crimes by identifying houses with expensive and easily resold items (Denning et al., 2013). The creation of wireless systems technology provides another vulnerability to enable tracking and reporting (Denning et al., 2013). Criminals are targeting modern homes because they now contain a wide range of new technology capabilities, and hackers can tap into these new technologies relatively undetected (Denning et al., 2013). Moreover, criminals have

compromised police cruisers by hacking into their onboard computer systems and streaming live video feeds as officers responded to incidents (Denning et al., 2013).

Financial crime committed in the cyber financial world is an emerging threat, particularly in online gaming where committing fraudulent activities goes virtually undetected (Keene, 2012). Moreover, due to lack of legislation and regulation, criminals are able to conceal real life crimes like fraud, identity theft, and money laundering using virtual worlds (FBI, 2013b; Keene, 2012). In cyber virtual worlds, users pay with genuine currency to modify their characters (Keene, 2012). Online gamers who converted their virtual dollars into genuine currency spurred several recent financial crimes (FBI, 2013b; Keene, 2012). Both the FBI (2013b) and Keene (2012) reiterated the need to establish legislative or regulatory clarification of the ambiguous lines between virtual and real-life environments since virtual environments continue to be an unmonitored criminal safe haven.

Developers of the emerging augmented reality (AR) glasses industry have created additional cloud computing security issues (Hyman, 2013a). AR glasses are wearable computer devices developed by Google Glass, Microsoft Corporation, and Apple Incorporated with an expected industry market of \$240 billion (Hyman, 2013a). Hyman (2013a) reported the concept behind AR glasses is to capture and collect everything you see and say and backup or save the data to cloud storage in real time. Subsequently, search engine giants like Google or Bing could buy the data to assist their respective companies with advertising (Hyman, 2013a). Security experts are concerned about the amount of data sold to third parties, as well as the issue of saving and backing up real

time data to the cloud, and predict a sharp increase in hacking along with the potential unauthorized surveillance use of AR glasses affecting individuals' rights (Hyman, 2013a).

Researchers are exploring and leveraging quantum mechanics to generate potentially unhackable communications because of the cyber espionage committed by Eric Snowden, a civilian contractor working for the National Security Agency [NSA] (Mone, 2013). To achieve the goal, Laurie and Doctorow (2012) proposed using a cryptographic protocol called sovereign keys (SK) instead of CAs, while Mone (2013) recommended using quantum cryptography utilizing photons in communication protocols versus the public-key cryptography. Financial institutions and various government entities are also evaluating future uses for quantum cryptography (Mone, 2013). Laurie and Doctorow encouraged browser vendors to adopt cryptographic protocols as a new security mechanism with the intention of creating a safer Internet environment.

Security awareness and malware identification are critical components to prevent cyber attacks and cyber crimes (Huang, 2013; Tchakounté, 2014). Tchakounté (2014) reported malware, viruses, and spyware are prevalent on computers, and currently infiltrating the operating systems, which support tablets and mobile devices. Huang (2013) articulated the botnet is one of the most notorious threats to Internet users. Likewise, Jang-Jaccard and Nepal (2014), Nagunwa (2014), and Prayudi and Yusirwan (2015) reported malware is one of the most serious threats associated with cyber security.

Nagunwa (2014) reported 556 million global online consumers were victims in more than 30 million hacking activities yielding economic losses exceeding \$110 billion.

Brute force, malware botnets, and web app attack are the prominent types of cyber attacks in the cloud environment (Singh, 2014). Nagunwa reported Trojans are the most deployed malware by phishers, accounting for 77% of all malware attacks whereby phishers install malware to steal credentials or link the host system to a botnet. Botnets have globally infected hundreds of millions of computers without the owners' knowledge (MacEwan, 2013; Nagunwa, 2014; Singh, 2014). Botnets infected with malware and malicious software have been increasing in numbers, are becoming more sophisticated, are extremely difficult to detect, and are almost impossible to stop (Jang-Jaccard & Nepal, 2014; MacEwan, 2013; Nagunwa, 2014).

Moreover, the botnet malicious invasion will continue to adversely impact SME owners who fail to recognize the threats and implement proper security strategies (MacEwan, 2013). The Stuxnet malware spied on and invisibly changed data for years hiding the cause of the Iran nuclear weapons centrifuge failures (Bambauer, 2013). Sophisticated malware succeeded where diplomacy and threats of military force failed (Bambauer, 2013).

Malware is often a mechanism for cyber criminal activities because malware characteristics usually elude most forensics experts' detection and analysis methods (Prayudi & Yusirwan, 2015). Prayudi and Yusirwan (2015) reported an infected application could potentially affect thousands of devices prior to its discovery. To combat malware exposure, computer, tablet, and mobile users must become more knowledgeable about protecting their devices, invoke limited permission grants by not

allowing the applications to access sensitive user information, and prevent exposure to cyber criminal activities (Tchakounté, 2014).

Business owners must find security critical computer bugs, more commonly known as software errors or flaws, in a computer program or system before hackers and cyber terrorists exploit the breached systems (Avgerinos et al., 2014). Likewise, NIST (2015a, 2015b) recommended business owners keep cyber security as a top priority as they explore opportunities created by mobile and cloud computing particularly since the proliferation of mobile devices connecting business networks has expanded the number of potential targets for cyber attacks. SME owners whose core competencies do not include IT can benefit from cloud sourcing, since they can essentially outsource their IT to an external provider (Dillon & Vossen, 2015). Additionally, cloud solutions are attractive for a number of reasons including ease of use, pricing, availability, scalability, and reliability (Dillon & Vossen, 2015). Implementing preventative solutions will help SME owners reduce risk exposure and possible security breaches (NIST, 2015a, 2015b).

Recent trends of unethical Internet activity reflect instances where the social media incited hatred and unrest, especially against government and law enforcement authorities (Salman, Saad, & Ali, 2013). Jang-Jaccard and Nepal (2014) maintained the exponential growth of the global Internet interconnections has led to an increased number of cyber attacks. There is a need for government authorities to develop a set of guiding principles to thwart unethical Internet abuse and law enforcement authorities to develop methodology for legal enforcement (Salman et al., 2013).

SME owners have become a target for criminals looking to access sensitive data because they have limited resources dedicated to information system security (SBA, 2014). The direct correlation to the finding is SME owners with no cyber security policies are even more susceptible to exploitation (SBA, 2014). An SBA (2015) research study encompassed four types of e-mail messages and correlated personal staff responses to each message. The SBA (2015) reported each study participant was knowledgeable on computer security yet still felt victimized by e-mail phishing and cyber exploitation exercises. In addition, researchers conducting the study investigated information assurance issues with SME owners to determine if there were any relationships between leadership styles and security policies enabling SME owners to prevent cyber crime activity (SBA, 2015). Researchers concluded SME owners needed to broaden their leadership styles to find cost-effective approaches to preventative measures (SBA, 2015).

Cyber attackers can gain access to networked or wireless items from anywhere on the Internet further substantiating the requirement for intrusion detection systems (IDS) to detect intruders and prevent cyber attacks (Kim & Park, 2013; Raza et al., 2013). Researchers reviewed and analyzed achieving maximum security results by implementing SVELTE, a new IDS, which claims to detect all malicious nodes on Internet Protocol version 6 (IPv6) over Low-power Wireless Personal Area Network (6LoWPAN) networks (Raza et al., 2013). Julisch (2013) reported anomaly detection systems are incredibly powerful tools for gaining situational awareness by reporting deviations from normal behavior rules and policies. Additionally, B. H. Kim and Park (2013) proposed a control system using a DNS firewall, which provides random client

access to the site for acts, which can block potential intrusion concerns thus reducing abnormal packets by 14%.

Cyber crimes. In the past criminals were able to go into businesses with guns and demand money. Today, criminals also digitally steal data. The tools and techniques for launching future cyber warfare attacks are the same as for cyber crime; however, the motives differ from political conflicts, undercover activities, and propaganda campaigns to financial objectives (FBI, 2015a, 2015b).

Kshetri (2013) discussed cyber attacks in China where there are more than 538 million Internet users and reported 45% were victims of malware attacks, 22% had their online accounts hacked, and 8% were victims of scammers. Symantec Corporation reported in their latest 2013 study that cyber crimes cost companies \$110 billion a year, whereas McAfee, Symantec's closest competitor, reported cyber crimes were 10 times more than what Symantec Corporation reported costing companies over one trillion dollars a year (Hyman, 2013b; Symantec Corporation, 2013). Although these studies reflect the exponential increase in cyber crimes and reinforce the requirement for SME owners to develop effective and preventative strategies, Bambauer (2013) recommended a different approach requiring the federal government to combine funding and legal mandates to push firms to redesign their computer systems.

Computer security. Cyber crime losses in 2012 were more than \$100 billion annually and increasing, and Filshinskiy (2013) argued criminals are more likely to commit crimes by selling their services via cyber criminal employment portals than by foreign adversaries paying hackers to infiltrate websites for national secrets. For

example, (a) hackers' rates for a DoS on a website ranged from \$50 to \$500 per day; (b) hacking into a private e-mail address ranged from \$30 to \$50 per address; (c) hacking into databases with backdoor passwords sold for \$250; and (d) hackers who sold their own custom malware for initial application plus monthly consultation fees, maintenance, and support charged \$1,500 (Filshinskiy, 2013). Additionally, a person does not have to be a criminal or hacker to inflict cyber losses--a skilled project manager within a company could easily profit from and inflict untold financial harm from cyber employment portals (Hua & Bapna, 2013).

Researchers have conducted several studies to determine whether there are common characteristics motivating hackers' behaviors, how hackers get started, and how and why they evolve from innocent behavior to criminal acts (Xu et al., 2013). Research reports stated the epidemic of computer hacking is a direct result of advances in computer networking technologies, such as the Internet, and extensive use of computers throughout society (Xu et al., 2013). Some computer hackers simply do not start out as delinquents or social deviants but often as curious and respected students fascinated by computers who transform into hackers by association with like-minded peers, accepted tolerance by teachers and school administrators, and their abilities to penetrate software barriers (Xu et al., 2013).

In fact, the only reliable differentiators Xu et al. (2013) found between grey hat and black hat hackers appeared to be their moral values and judgment. The Communications of the ACM (CACM) Staff (2013) extended Xu et al.'s research by discovering additional hacker motivations and concluded malicious hacking motivations

have not changed since the 1960s. Malicious hackers intended to achieve their goals through mischievous means by causing harm to others, and some young hackers are looking for shortcuts to very profitable careers without having to attend formal schooling (CACM Staff, 2013). Likewise, younger participants were more likely to engage in both hacking and malware-related behaviors, suggesting there may be an age-crime curve relationship present for cybercrimes (Chua & Holt, 2016).

Additionally, Chua and Holt (2016) conducted a study to determine whether there are relationships between the techniques of neutralization focused on rationalizing action and neutralizing guilt, computer hacking, and malware use behaviors amongst college students from South Africa, Taiwan, and the U. S. Chua and Holt (2016) discovered the relationship between all three techniques of neutralization were significantly associated with both simple hacking and malware-related behaviors. These discoveries validate the need to develop and utilize preventative measures to combat these behaviors to influence and transform hackers' behavioral motivations from causing harm.

Security awareness. Security awareness in the cyber environment enables organizations to make better decisions to protect their data. Cyber crimes have increased at an alarming rate resulting in devastating impacts on the national security and economy (FBI, 2013a). Widespread exposure provides hackers access to individual and company sensitive information to achieve criminal gains (Grossman, 2013). The reality is while regulation is a necessary part of the legal system, cyber space regulations must be flexible and adaptable to address opposing threats (Bambauer, 2013).

Researchers evaluated seven articles related to situational crime prevention and routine activity theory and their application to issues of organized crime and terrorism (Kleemans, Soudijn, & Weenink, 2012). Special characteristics and motivation explain organized crime activity, and investigators use situational crime analysis to help identify circumstances, which facilitate crime (Kleemans et al., 2012). Imposing situational analysis on organized crime efforts generates opportunities for crime prevention, and criminal investigators are essential to preventing organized crime and terrorism activity (FBI, 2015a).

Son and Jeong (2013) discussed society's increasing utilization and dependency on the Internet and the dangers associated with intrusion threats by computer hacking, malicious code, and viruses. Users must learn hacking principles to recognize security threats and potentially prevent a cyber hack (Hong, Kang, Kim, & Park, 2013). Business owners are especially vulnerable and defenseless when exposed to cyber attacks if they host their data on a third-party's single server (Son & Jeong, 2013).

Egele et al. (2012) provided a comprehensive overview of malware and different analysis techniques users can implement to prevent potential malware threats on their computers and mobile devices. Malware is software, which is deliberately harmful upon attack and includes multiple types, such as a worm, virus, bot, spyware, rootkit, and a Trojan horse, each with the ability to hide certain information and wreak havoc on user systems (Egele et al., 2012). Antivirus vendors commonly receive thousands of malicious samples daily as malware threats and attacks increase (Egele et al., 2012;

Tchakounté, 2014). These exploitations usually result in significant loss of information and data and potentially pose serious financial loss.

The most common malware attacks result from weak remote administration or VPN authentications (Bodhani, 2013). Business owners could mitigate against zero-day malware attacks by using a new emerging technology called whitelisting (Shahzad, Hussain, & Khan, 2013). The whitelisting technique is simple and lightweight, leverages existing blacklisting techniques, and allows legitimate services, processes, websites, and trusted applications to run on a selected device while preventing other threats (Shahzad et al., 2013).

Hackers use millions of malicious web links to distribute and propagate malware over the Internet, and traditional security technologies are limited in their capability to mitigate malware issues (Chang, Venkatasubramanian, West, & Lee, 2013; Tchakounté, 2014). Chang et al. (2013) reported researchers analyzed various web based malware attacks to determine the type of attack model, the cause, and the vulnerabilities, which enabled the attack. The research analysis identified three categories to analyze, identify, and defend a malware infection each with its own advantages and disadvantages, which are dependent upon the selected implementation strategy (Chang et al., 2013).

Many well-known companies are in the forefront against computer hacking attacks and threats (Sheldon & McDonald, 2012). Motivated individuals and groups have also begun targeting high-profile Internet companies and their websites thus exposing security flaws. The highly publicized Sony attack illustrated new security hacking dangers when hackers obtained Sony user data comprised of Sony PS3 usernames,

passwords, bank accounts, and credit card numbers (Sheldon & McDonald, 2012).

Conversely, Sony reported encrypting users' credit card data, but their passwords were not encrypted placing customers who reused the same passwords on other sites in jeopardy (Bambauer, 2013). Additionally, Bambauer (2013) reported Sony received a backlash from users since they did not immediately notify users of the data breach.

Investigators assessed U.S. Fortune 500 corporations' retail e-commerce security status using quantitative analysis to identify their strengths and weaknesses for improvement (Zhao & Zhao, 2012). Investigators used content analysis, information security auditing, and network security mapping for data collection and analysis, which indicated most sites posted security policies; however, only one-third provided details on which security measures were implemented (Zhao & Zhao, 2012). Additional data analysis revealed many of the e-commerce sites secured user *My Account* login with Secure Sockets Layer (SSL) encryption but only 16% invoked lockout after using three failed attempts (Zhao & Zhao, 2012). Although the e-commerce sites had most of their Internet ports filtered or behind firewalls, almost one-third of the e-commerce sites' computer operating systems were detected from several open ports, enabling security breaches or holes to be exploited by cyber attackers (Zhao & Zhao, 2012).

Moreover, Haichang, Wei, Fei, and Licheng (2013) reported the results of a study focused on security aspects of existing graphical password schemes, proposed enhancements for two-factor authorization, and examples of current cyber attack methods. Researchers categorized existing graphical password schemes into four types based on authentication style, and provided a comprehensive introduction and security

analysis for each scheme. Additionally, researchers categorized known attack methods into two types, and based on phishing, pharming, or spyware attack, summarized security password schemes used to achieve cyber attacks (Haichang et al., 2013).

Geer (2013) discussed his view about society's global dependency on the Internet and the quest for real time instant information. The Internet, phones, tablets, watches, and a multitude of products are dependent upon technological availability and reliability. Geer argued 90% of the U.S. population has become dependent on the Internet and the embedded services requiring the need to ensure some level of manual capability to continue normal operations. In case of a catastrophic event, data users must have a contingency plan to recover their information.

Goldsborough (2012) stated there are multiple storage solutions, such as external hard drives, universal serial bus (USB) devices, compact disk-read only memory (CD-ROM) disks, and several cloud providers who provide free cloud backup and storage. Despite having multiple solutions available, Goldsborough argued one of the biggest concerns is for users to utilize the available solutions. The Internet is considered critical to the global infrastructure and yet is not adequately protected (Geer, 2013; The White House, 2014).

Fraudsters are business people who commit fraud for a living and are prepared to invest time and money to create conditions where they can implement fraudulent activities because the benefits are enormous (Yelland, 2013). Fraud methodologies will always exist; the method of attempting to thwart them needs exploitation. Most people think of mobile fraud as having a cell phone stolen or hacked; however, Yelland (2013)

identified seven types of basic fraud typically occurring in mobile networks. Businesses lose approximately \$60 billion a year due to fraud and lack of effective revenue protection, which dwarfs in comparison to the issues around personal security, which network operators suffer and often fail to acknowledge (Filshtinskiy, 2013; Yelland, 2013). Consumer advocacy groups promote increasing user and business awareness and taking steps to reduce risk exposure (DHS, 2015a; FCC, 2014; SBA, 2014).

White hat hackers or crackers are individuals who break into computer security systems, not for malicious nor personal gain, to identify security weaknesses and vulnerabilities within computer systems (Fulton, Lawrence, & Clouse, 2013). Employers are searching for college graduates who possess specific technical and social skills to enter the cyber industry career field (Fulton et al., 2013). The thousands of cyber attacks occurring daily highlight the need for a workforce with the requisite skills and sufficient size to meet the growing demands (Burley, Eisenberg, & Goodman, 2014).

Global technology is a valuable commodity to people, businesses, and governments (The White House, 2015b). Although the Internet has transformed the entire global society by enabling information sharing and spurring economic prosperity, cyber criminals continue to find creative ways to penetrate laptops, phones, and computer networks resulting in numerous cyber security attacks and thefts (Tchakounté, 2014). The key to effective cyber security is the management of organizational risk (FBI, 2014, 2015c). Companies should invest in securing their data to prevent financial loss due to network hacking and security breaching by users whose sole purpose is to gain access based on a user's or system's weakness (DHS, 2015a; FBI, 2015c).

Hackers have unlimited access to the Internet via compromised computers because the bogus certificates appear to be authentic (Laurie & Doctorow, 2012). SME owners are particularly vulnerable to cyber attacks, must be knowledgeable of potential attack areas, and develop strategies to mitigate inadvertent company exposure to cyber attacks (SBA, 2014, 2015). The global economy depends on effective cyber security strategies to ensure individuals', businesses', and global governments' infrastructure assets remain secure (FBI, 2015a; Shackelford et al., 2015). While multiple factors influence SME owners' decisions to establish and implement cyber security protection strategies and implementation plans, the literature review substantiates the need for SME owners to be aware of cyber security threats, then develop and implement effective strategies and preventative measures to combat cyber crimes and ensure their continued success.

Transition

Section 1 was an introduction, which described the background of the doctoral study of cyber security attack phenomena, and preventative measures SME owners employed to hinder cyber attacks. Section 1 encompassed 12 major elements, which provided the doctoral study's overall foundation and scope. Critical areas within the section included a background of the problem; the problem statement; the purpose statement; nature of the study; research questions; conceptual framework; operational terms; assumptions; limitations; delimitations; the significance of study; and summarization of professional and scholarly works of literature.

Cyber attacks have many forms ranging from hacking, viruses, and Trojan horses, to worms on desktops, tablets, mobile devices, automobiles, and home appliances. The global economy depends on effective cyber security strategies to ensure individuals', businesses', and global governments' infrastructure assets remain secure (FBI, 2015a; Shackelford et al., 2015). Cyber crimes have no boundaries fueling cyber criminal activities, and potential occurrences for cyber attacks grow daily (FBI, 2015a). Security awareness, prevention, and proactive actions can mitigate and possibly alleviate future cyber attacks on small businesses.

Section 2 restates the purpose statement; provides new subsections expanding on the roles of the researcher and participants; the research method and design; population and sampling criteria; ethical research criteria; data collection instrument and techniques; data organization and analysis methodologies; reliability and validity criteria mechanisms; and transitions into Section 3. Section 3 provides the detailed data collection analysis of the multicase doctoral study.

Section 2: The Project

Cyber security experts have reported that incidences of cyber crimes are on the rise and increasing daily as savvy and persistent information communication attackers find creative ways to penetrate laptops, phones, computer networks, and anything considered a wired device (FCC, 2014; Gootman, 2016). My objective in this study was to explore the effective cyber security strategies SME owners utilized and how these activities potentially reduced cyber threats.

Purpose Statement

The purpose of the qualitative multicase study was to explore effective strategies SME owners used to protect their businesses from cyber attacks. The specific population consisted of four SME owners operating in the Melbourne, Florida area who utilized the Internet for business operations. Additional selection criteria for the study required that SME owners (a) were licensed to operate a retail business in Melbourne, Brevard County, Florida; (b) employed between one and 249 personnel; (c) had an annual gross revenue under \$10 million; and (d) had successfully implemented cyber security strategies.

Given the findings reported by the National Cyber Security Alliance (NCSA, 2015) and in the U.S. House of Representatives Committee on Small Business hearing on “protecting small businesses against emerging and complex cyber-attacks” (2013), I determined that the selected population in this study was appropriate because 60% of SMEs go out of business within 6 months after the first cyber attack. Findings from my study may provide SME owners effective strategies to protect against a cyber attack, which may increase consumer confidence and result in greater economic prosperity for

the local community. SME owners who have survived cyber attacks might spur economic growth by employing residents of the community, fueling the socioeconomic lifecycle.

Role of the Researcher

Qualitative researchers assume several to gather data from participants by using document reviews, personal interviews, and observations (Sangster-Gormley, 2013; Snelgrove, 2014; Yilmaz, 2013). Qualitative researchers effectively (a) develop themselves into research instruments capable of collecting data from a representative sample; (b) develop, interpret, and complete qualitative data analysis; and (c) present study findings while adhering to high quality research and ethical standards (Alshenqeeti, 2014; Marshall & Rossman, 2016; Pacho, 2015). I was the interviewer and primary data collection instrument for the four study participants obtained through the purposive snowball sampling strategy.

I live in southeast Florida and am an executive manager and a subject matter expert in information technology practices, program management, and system methodologies. I did not have a professional relationship with the study participants. These factors may have mitigated the participants' concerns about revealing sensitive information or possible reluctance to participate in the study. In this multicase study, I explored the issue of whether cyber security protection strategies are beneficial for SME owners and sought to determine any benefits.

Qualitative research protocols include clearly delineating the study's problem, background, rationale, objectives, research design and methodology, data analysis, and

organization (Marshall & Rossman, 2016; Patton, 2015; Yin, 2014). The U.S. Department of Health and Human Services (DHHS) provides human subjects research protocols and guidelines, and the Belmont Report mandates adherence to three fundamental ethical principles when conducting research with human participants: respect for persons, beneficence, and justice. Mandatory ethical compliance requires researchers treat individuals as autonomous agents and provide them with additional protection (Brody, Migueles, & Wendler, 2015; DHHS, 1979).

Researchers must treat participants in an ethical manner, protect them from harm, and ensure their safety and well-being. Mandatory ethical compliance requires researchers use fair procedures and outcomes to select participants, and ensure there is an equitable distribution of benefits and burdens to the population sample (Brody et al., 2015; DHHS, 1979). Adherence to these guiding principles provides an ethical foundation for conducting research with human participants. The most valid form of qualitative data collection is personal interviews since they capture human interactions and emotions (Marshall & Rossman, 2016; Morse & McEvoy, 2014; Pacho, 2015; Yin, 2014). I adhered to the ethical principles and guidelines for the protection of human subjects as described in the Belmont Report while conducting this multicase study research.

Qualitative researchers have an advantage over quantitative researchers inasmuch as they can add new pieces to the research puzzle, or entire new puzzles can be conjured while they gather data in both the collection and analysis phases (Pacho, 2015). Smith and Noble (2014) indicated bias might occur in the planning, data collection and analysis, or

reporting phases of research. Understanding research bias allows critical and independent review, thus avoiding potentially damaging actions. A case of human decision bias is automation bias, a decision aid that provides incorrect advice (Wickens, Clegg, Vieane, & Sebok, 2015). Wickens et al. (2015) reported that when humans depend on automation, they might manifest the automation bias with wrong advice, triggering lost accuracy, and manifest complacency with wrong advice. Additionally, Egidi (2015) stated that cognitive science has demonstrated that human behavior, beliefs, and attitudes are automatic and generate unconscious rational processes.

Educational guidance on adapting and integrating unconscious bias helps students identify, reduce, and manage unconscious bias by encouraging change once a bias is recognized (Allen & Garg, 2016). To mitigate bias in qualitative research, researchers should (a) understand research limitations, random sample populations, and the demographics of participants; (b) maintain participant anonymity; (c) eliminate experimental data errors by reviewing and validating data; and (e) accurately record the findings (Lunnay, Borlagdan, McNaughton, & Ward, 2014; Smith & Noble, 2014). To mitigate biases, I (a) adhered to ethical research practices, (b) focused on the context of the study, (c) participated only as an outsider, (d) adhered to the interview protocol, (e) protected the privacy of participants, (f) maintained the confidentiality of the data, (g) guided the conversation and refrained from leading questions, (h) avoided reactions based on respondent responses, (i) objectively interpreted data obtained from participants, (j) utilized member checking, and (k) maintained an audit trail during the research process.

In addition to research protocols, researchers should also develop interview protocols to guide them through the entire interview process (Marshall & Rossman, 2016; Patton, 2015; Yin, 2014). Exposing the human story is essential in qualitative research, and interviewing is a method that enables researchers to gain insight into participant stories. Successful interview protocols include a variety of elements: an interesting research topic, prior research knowledge, and a good interview script. In semistructured qualitative research interviews, the richly detailed discussion between participant and researcher is better achieved via face-to-face interviews rather than through telephone interviews (Irvine, Drew, & Sainsbury, 2012; Smith & Noble, 2014).

Interviewers must be aware of participants' body language and facial expressions, and must display genuine interest and concern throughout the interview. I used the study interview protocol (see Appendix D) to designate the parameters for the interviews and set the participants' expectations. The detailed interview protocol specified I would (a) be conscious of facial expressions, body language, tone, and dress to not introduce bias with respondents; (b) remain neutral in my body language, facial expressions, and tone; (c) ask questions without leading respondents, (d) refrain from offering my opinion, (e) strive for objectivity by recognizing my personal biases, and (f) report the collected data without prejudice.

Participants

Qualitative researchers select their sample size in an arbitrary fashion (Marshall et al., 2013). Moreover, Cronin (2014) and Onwuegbuzie and Byers (2014) reported that while a minimum of four to 15 participants is desirable, the primary focus is on gathering

thick, rich data and not on the number of participants. In 2012, there were 7,518 businesses in Melbourne, Florida, indicating a sizable population from which to draw a representative sampling of SME participants (U.S. Census Bureau, 2015). I conducted sampling of four for-profit SME owners who used the Internet for business operations, had successful cyber security strategies to protect their businesses from cyber attacks, and were located within a 5-mile geographic area in Melbourne, Brevard County, Florida. SME owner selection criteria consisted of each of the following (a) were licensed to operate a retail business in Melbourne, Brevard County, Florida; (b) employed between one and 249 personnel; (c) had an annual gross revenue under \$10 million; and (d) had successfully implemented cyber security strategies.

Participant recruitment requires innovative strategies and involves leveraging trusted relationships to get past gatekeepers and gain access (Pattinson & Preece, 2014). According to Brooks and Normore (2015), a noticeable omission in many qualitative research studies is a lack of attention to the relational, power, and gatekeeper dynamics that influence the study. Moreover, the process of negotiating with gatekeepers requires time to build trust, establish a shared understanding, and develop a commitment to the objectives of the research study (McAreevey & Das, 2013). In multicase studies of small businesses, the gatekeepers are typically the small business owners; however, they may be prominent figures working for the owners.

The Internet is a viable research medium for mitigating access and distance issues (Deakin & Wakefield, 2013; Gothberg et al., 2013; Lunnay et al., 2014). To gain access to participants, I used a four-phase methodology: preentry, formal contact, fieldwork, and

post fieldwork. Internet searches of online business directories, tax records, and government agencies' websites provided the best sources of potential participants. I petitioned selected SME owners through e-mail, telephone, and social media avenues such as Facebook, and generated appointment requests based on the participants' availability within a specific timeframe.

A key principle researchers must adhere to before gathering participant data is informed consent (Lunnay et al., 2014). In the official correspondence (see Appendix B), I emphasized the benefits of the research, requested informed consent, ensured the prospective participant's confidentiality, and requested permission to record the interview. Research integrity requires upholding ethics while conducting qualitative research (Irvine et al., 2012). For the fieldwork phase, researchers have stressed the importance of dressing appropriately, arriving on time for interview appointments, and monitoring and maintaining neutrality with body language and facial expressions (Irvine et al., 2012).

Social media is another mechanism to facilitate communication with participants (Lunnay et al., 2014). Deakin and Wakefield (2013) reported that using the Skype communication service offers researchers an innovative interview method to collect qualitative data. According to Janghorban, Roudsari, and Taghipour (2014), using a free synchronous method of communication service such as Skype in research provides an alternative to obtaining interactive face-to-face interviews by calling, seeing, messaging, and sharing with people wherever Internet capability exists. In the post-fieldwork phase, I sent each participant a formal thank-you note via email.

Additionally, member checking concluded within 2 days of receipt of the data interpretation file from the interview session. Participants who failed to respond within the specified timeframe agreed with the data accuracy and provided complied consent. Finally, if there was insufficient data collected or additional clarification required, I contacted participants to clarify any anomalies.

Qualitative researchers seek to answer questions versus testing a hypothesis. Onwuegbuzie and Byers (2014) explained interviews are the most common source of data in qualitative research. Qualitative interviewers engage in active listening involving probing and phrasing to develop trust, rapport, and facilitate more in-depth discussions (Rossetto, 2014). The approach to establishing a working relationship with project participants began by initial contact with each small business owner through the company's website or direct e-mail. The success of the qualitative interview is contingent on how well the researcher establishes rapport with participants; establishing rapport and mutual respect requires meetings over time between the interviewer and each participant (Bowden & Galindo-Gonzalez, 2015).

Lunnay et al. (2014) described interactions using social media and identified several potential risks when used as a facilitation method. Trust and shared understanding are equally critical areas in which to develop a rapport with participants when conducting qualitative interviews (Abbe & Brandon, 2013). Developing a rapport with participants as quickly as possible enables the respondents to feel they can engage in honest and candid discussions. Before conducting the initial meetings, I conducted research to gain insight on the prospective participants' businesses.

Manning (2014) discussed the impact of interpersonal communication research by expanding inquiry as not only a tool for expressing social reality but as a device to produce it. It is critical during initial meetings with participants to establish rapport and determine their willingness to participate in the uncompensated research study. Once the SME owners voluntarily agreed to participate, then both parties coordinated the dates, times, and locations for interviews. To develop rapport, I (a) established a mutual feeling of friendliness and highlighted common interests; (b) described the research topic, my interest in the study, answered questions, and put participants at ease; (c) reassured participants of data integrity throughout the process; and (d) reemphasized confidentiality. Additionally, I (e) interacted in a positive, professional manner; exhibited politeness and good manners, and maintained a nonjudgmental attitude to ensure positive working relationships; and (f) showed attentiveness by actively listening and engaging with interviewees throughout the sessions.

Research Method and Design

Qualitative, quantitative, and mixed methods are the three paradigms used for conducting research (Marshall et al., 2013; Mayoh & Onwuegbuzie, 2015; Poni, 2014). Phenomenology, ethnography, and case study are three types of qualitative designs (Baškarada, 2014; Marshall et al., 2013; Yilmaz, 2013; Yin, 2014). The study utilized the qualitative research method and the case study design approach to explore the effective strategies SME owners used to protect their businesses from cyber attacks.

Research Method

Researchers select a method based on research objectives and rationale for the study. Brooks and Normore (2015) emphasized one of the most important processes a qualitative researcher undertakes is selecting an appropriate research design and then adapting it to suit the specific context of the study. Choosing a design methodology requires multiple criteria, which include objectives for study, research questions, data collection, and timeframe constraints. The research methods selected should be a simple, adaptable set of specific procedures and techniques to collect and analyze data (Houghton et al., 2015; Pacho, 2015; Yin, 2013).

In some instances, researchers combine two methods to achieve maximum results resulting in a mixed methods research approach (Azhar et al., 2013; Mayoh & Onwuegbuzie, 2015; Querstret & Robinson, 2013). Researchers utilize qualitative methods to explore contemporary, real life situations, understand the phenomenon, identify events' significance, answer questions, and capture the descriptive human experiences within their data collection methodology (Baškarada, 2014; Bridges-Rhoades & Van Cleave, 2014; Yin, 2014). In contrast, quantitative researchers pursue questions or hypotheses, which describe, categorize, or relate comparison groups to provide trend analysis on attitudes and opinions to explain and provide understanding to the social phenomena (Palinkas, 2014; Yilmaz, 2013; Yin, 2014).

Hazzan and Nutov (2014) described investigators primarily use qualitative research methods to study social phenomena, situations, and processes, which involve people perspectives. Sargeant (2012) summarized quantitative methods as research,

which focuses on the impact of an intervention and typically answers questions about its effectiveness. Alternatively, Trafimow (2014) suggested using qualitative methods in the exploratory period of the research project to determine the relevant variables, and then using quantitative methods to quantify how much the variables matter. Likewise, the mixed methods research methodology combines both qualitative and quantitative methods (Azhar et al., 2013; Mayoh & Onwuegbuzie, 2015; Querstret & Robinson, 2013).

Qualitative research methods are analytical, based on participants' experiences, occur in natural locations, and examine small groups of people for a specific timeframe (Bridges-Rhoades & Van Cleave, 2014). Quantitative researchers pursue questions or hypotheses, which describe, categorize, or relate comparison groups to provide trend analysis on attitudes and opinions to explain and provide understanding to the social phenomena (Palinkas, 2014; Yilmaz, 2013; Yin, 2014). Mixed methods research methodology capitalizes on the primary elements of qualitative design by describing the phenomena while utilizing quantitative design elements for statistical tests of hypotheses (Azhar et al., 2013; Mayoh & Onwuegbuzie, 2015). Mixed methods research leverages elements from both quantitative and qualitative methods creating a mixed strategy to investigate phenomena (Azhar et al., 2013; Mayoh & Onwuegbuzie, 2015; Tong et al., 2013). Mixed methods research methodology can provide breadth and depth of understanding phenomena while masking weaknesses of a selected research method (Mayoh & Onwuegbuzie, 2015; Morgan, 2014; Palinkas, 2014).

Frameworks assist researchers to ensure they have coherently framed the research throughout their design (Green, 2014). The objective of the study was to explore effective cyber security strategies SME owners used to protect their businesses from cyber attacks. Cyber attacks are significantly a new phenomenon with profound economic, political, and social consequences in local and global arenas. Qualitative research methods are more applicable to explore and determine phenomenon possibilities than quantitative or mixed methods research methods.

The qualitative method was most appropriate because the research intent was to explore effective strategies SME owners have implemented to deter cyber breaches. SME owners must analyze computer and network security vulnerabilities to determine effective security exploitations (Dunn Caveltly, 2014). To explore effective cyber security strategies, I did not investigate hypotheses, which are part of the quantitative study or the quantitative portion of mixed methods study but utilized the qualitative multicase study design to explore effective cyber security strategies SME owners used to protect their businesses from cyber attacks.

Research Design

Phenomenology, ethnography, and case study are three types of qualitative designs (Baškarada, 2014; Marshall et al., 2013; Yilmaz, 2013; Yin, 2014). Each approach contains similar aspects of research about the research problem, questions, data, data analysis, and reporting results; however; the data collection processes are entirely different (Gale et al., 2013; Mayoh & Onwuegbuzie, 2015; Yilmaz, 2013; Yin, 2014). Phenomenology is a design method for qualitative investigation examining the meaning

of lived experiences of a person or group of individuals about a single phenomenon thus describing participants' collective experiences (Gale et al., 2013; Mayoh & Onwuegbuzie, 2015; Tuohy et al., 2013). Ethnography is a design methodology for qualitative investigation for studying people and cultures requiring researchers to observe participants in their natural habitats to gain a deeper understanding of how people experience, perceive, create, and navigate the social world (Hallett & Barber, 2014; Murthy, 2013; Perry, 2013). Case study is another qualitative design methodology which explores a bounded system over time through detailed, in-depth data collection, using multiple sources of evidence in rich context, within a real life framework (Baškarada, 2014; Boblin et al., 2013; Marshall et al., 2013; Yin, 2014).

I selected the qualitative multicase study design as the most suitable choice to explore what effective cyber security strategies SME owners used to protect their businesses from cyber attacks. Additionally, qualitative case study design incorporated my pragmatic worldview, systems theory conceptual framework, small sample population, data collection and analysis methods, as well as the time constraints to conduct a doctoral study within a specified timeframe. The phenomenology design was not the appropriate design choice because I did not explore lived experiences in the research. Similarly, the ethnography design was not a suitable design selection for the study due to lack of group culture observations.

Replication occurs when two or more cases support the same theory (Marshall et al., 2013; Yin, 2013, 2014). Data saturation occurs through a series of data collection events generating significant amounts of data from multiple resources, which fit diverse

experiences into predetermined response categories (Morse & McEvoy, 2014). Data saturation exists when no new information, concepts, or themes occur in subsequent interviews causing an interview redundancy (Cleary, Horsfall, & Hayter, 2014; Elo et al., 2014; O'Reilly & Parker, 2013).

Several factors determine saturation, and smaller studies may achieve saturation quicker than larger studies while controlling the size and scope of the case study assists with data saturation (Fusch & Fusch, 2015; Smith & Noble, 2014; Yin, 2014). To ensure data saturation in the study, I interviewed participants until no new data or knowledge emerged. Redundancy and lack of any new concepts or emerging knowledge from collected data confirm data saturation (Houghton, Casey, Shaw, & Murphy, 2013; Marshall et al., 2013; O'Reilly & Parker, 2013).

Population and Sampling

The multicase study research sample consisted of four small business owners located within a 5-mile geographic area in Melbourne, Brevard County, Florida, within zip codes 32901 and 32903, exploring decisions regarding successful SME cyber security strategies and practices. The data collection approach for the multicase study utilized the purposive snowball sampling strategy. B. Marshall et al. (2013) argued case studies are the most difficult type of qualitative research to classify since there are no rules for sample size in qualitative inquiry. Moreover, a population sample size depends on what the researcher wants to know, the purpose of the research, what will be useful, what will have reliability, and what elements are attainable within the timeframe and resources (Cleary et al., 2014; Cronin, 2014; Marshall et al., 2013).

Various experts provided opinions for the optimal case study sampling size ranging from four to 50. Yin (2014) recommended a minimum case study sample size of six while Cronin (2014) argued the research sampling unit for analysis varies from an individual to a group of people. Gentles, Charles, Ploeg, and McKibbon (2015) specified four to 10 was adequate for qualitative case study; however, ultimately the researcher determines the sample size based on the purpose of inquiry and the research question. Data saturation exists when no new data, concepts, or themes occur in subsequent interviews producing interview redundancy (Boddy, 2016; Cleary et al., 2014; Elo et al., 2014).

Data, investigator, theory, and methodological are several types of triangulation techniques used to support data saturation and validity (Denzin, 2012; Fusch & Ness, 2015; O'Reilly & Parker, 2013). Denzin (2012) discussed utilizing methodological triangulation techniques to assist and provide qualitative researchers an in-depth understanding of the phenomenon in the study. To ensure data saturation in the multicase study, I interviewed participants until no new data or knowledge emerged, and correlated data from multiple data collection methods. The data collected from the four participants met data saturation; therefore, no requirement existed to increase the sample size.

Defining the study sampling requires foresight and preparation about the requirements to gain insight into understanding the research topic. According to Grosseohme (2014), the study investigator establishes the criteria at the beginning to describe participant characteristics and helps determine how large and how diverse the sample needs to be. Moreover, Barratt, Ferris, and Lenton (2015) and Tong et al. (2013)

reported purposive sampling relies on the researcher's saturated knowledge of the field and rapport with members of targeted associations. Similarly, Palinkas et al. (2013) reported the snowball sampling strategy limits the range of variation and focuses on the study's similarities.

Qualitative researchers determine their sampling strategy to accurately depict the phenomenon, which focuses on capturing rich detailed participant experiences through small versus large sample sizes of respondents used in quantitative studies (Grossoehme, 2014). Qualitative research participants' sampling frames are purposeful rather than at random (Palinkas, 2014). Cleary et al. (2014) acknowledged member selection must be compatible with the study's conceptual framework.

The approach for the multicase study utilized a purposive snowball sampling strategy. There are no best practices for determining sample size; however, a minimum of four to 15 participants is desirable with the primary focus on gathering rich data versus the number of participants (Baškarada, 2014; Cronin, 2014; Marshall et al., 2013; Onwuegbuzie & Byers, 2014). The study sample consisted of four SME owners located within a 5-mile geographic area in Melbourne, Brevard County, Florida, within zip codes 32901 and 32903, and met the minimum number required to meet the project sample size for a qualitative case study. I conducted a purposive snowball sampling of four for-profit SME owners within a 5-mile geographic area in Melbourne, Brevard County, Florida, ensuring the sample size was representative of the population. Selection criteria for the study required that SME owners (a) were licensed to operate a retail business in Melbourne, Brevard County, Florida; (b) employed between one and 249 personnel; (c)

had an annual gross revenue under \$10 million; and (d) had successfully implemented cyber security strategies.

I started recruitment of the sample population by using published business statistics provided by state and local government agencies. The first search method consisted of queries within the SBA website, District 2, which covers Brevard County and Melbourne, Florida (SBA, 2014). Utilizing links on the SBA website, information on the multiple small business programs provided the initial source for obtaining business listings, which met the population's sample criteria.

The second search method accessed small business listings utilizing the business resource guide obtained through the Melbourne Regional Chamber of East Central Florida Internet and City of Melbourne websites (Brevard County Tax Collector, 2014; City of Melbourne, 2016; Melbourne Regional Chamber of East Central Florida, 2016). The third method provided access to SME owners within the Brevard Small Business Assistance Council (BSBAC), whose primary purpose is to promote small business growth in Brevard County (SBA, 2016b). The next method accessed SME owners listed on the Space Coast SCORE website (Space Coast Score, 2016). Finally, attending the monthly Brevard County Economic Development Commission (EDC) meetings provided another access point to SME owners who are networking throughout the county seeking business growth and opportunities (EDC, 2016). To scope the effort, search criteria consisted of mailing zip codes 32901 and 32903 within the Brevard County Tax Collector's database (Brevard County Tax Collector, 2014). Limiting search criteria to two zip codes provided a sufficient number of participants matching the study

population's criteria to reach data saturation; therefore, no requirement existed to expand the geographic search.

Qualitative research emphasizes the importance of evaluating phenomenon when it takes place in its real-world setting (Yin, 2014). The case study design investigates a phenomenon in its natural setting where control or manipulation of participants is not likely (Abma & Stake, 2014; Tsang, 2014; Yilmaz, 2013; Yin, 2014). Likewise, researchers recommend considering the participant's interview preference settings to improve rigor and validity (Yager, Diedrichs, & Drummond, 2013). A relaxed interview setting allows participants to respond freely and ask questions (Scheibe, Reichelt, Bellmann, & Kirch, 2015). The familiar setting where the participants feel comfortable, secure, and at ease to discuss their points of view allows interaction with the investigator without changing the natural environment. Selected research participants were SME owners who could provide insightful information about the research topic.

The interview setting was in a private location to minimize distractions, ensure privacy, and avoid intentional automation bias. During the interview, both the interviewer and participant avoided external distractions by turning off mobile devices. I conducted semistructured interviews in person at the agreed upon locations using the SME Owner's Cyber Security Strategies Interview Questions (see Appendix A) to explore participants' experiences related to cyber security practices. Audio recording the interviews captured the context, questions, and answers, and allowed me to maintain eye contact with the participants and focus on the specific data collection. After each interview, the participants asked questions and provided additional data. Appendix D

contains the interview protocol which ensured the interviewer asked each participant the same questions in the same sequence during each interview.

Ethical Research

Before embarking on any doctoral research project, researchers are required to complete ethical standards training. Moreover, dependent on the type of research, specific ethics, and quality of research training might also be required. Ethical obligation arises out of the principle of beneficence, which requires researchers to minimize harm to study participants, and respect for persons (Wolf et al., 2015). To ensure ethical compliance, I (a) adhered to ethical research practices, (b) obtained informed consent, (c) protected the privacy of participants, (d) maintained the confidentiality of the data, (e) discussed the withdrawal process, (f) obtained statements of cooperation to record interviews, (g) secured and encrypted soft copy data, and (h) will retain both the soft copy and hard copy data for 5 years in a lockable cabinet in my home.

Consenting Process

Nishimura et al. (2013) stated informed consent is a critical component of ethical human participant research studies and guidelines for research informed consent should be cost effective for researchers and institutions to implement. The informed consent procedure protects the rights of participants and upholds the ethical value of participant autonomy (Chiumento, Khan, Rahman, & Frith, 2015). Walden University's IRB approval number for this multicase study is 12-05-16-0413975. I followed the recommendations for research ethics and standards provided by the National Institutes of

Health (NIH) and satisfactorily completed the required training course on protecting human research participants before submitting the doctoral study for review.

1. Confidentiality was a critical element of the qualitative design and ensured no identification or reporting of individual organizations or persons.
2. All study participants provided written consent.
3. Participants could withdraw without penalty from the study at any time by notifying the researcher via e-mail, telephone, or in person.
4. Participation was strictly voluntary; there was no paid incentive for study participants.
5. Maintenance of collected study data in a secure place for 5 years will protect the rights of participants.
6. There were no anticipated or direct benefits to the participants: the resulting data analysis may benefit society.

Participant Withdrawal Process

The selected SME owners had the right to decide whether to participate in the doctoral study using the informed consent process and could withdraw without penalty at any time. Participants could withdraw from the study at any point via e-mail, telephone, or in person expressing their desire to withdraw from the study. No study participant has requested to withdraw. To maintain an audit trail for replication and ensure data reporting integrity, I will retain electronic encrypted and paper data files, including a sample of the coded reflection journal and research log, in my home in a locked file

cabinet for 5 years per university requirements and after the 5 year period, shred all study data.

Measures for Ethical Protection

The multicase study excluded retail business owners employing more than 249 employees or with annual gross business revenues exceeding \$10 million. Researchers have a corresponding ethical and legal obligation to maintain the confidentiality of collected data and typically promise in consent forms to restrict access and conceal identifying data (Alshenqeeti, 2014; Wolf et al., 2015). Moreover, federal regulations govern human subjects' research by imposing an obligation on institutional review boards (IRBs) to ensure adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data prior to approving a study (Wolf et al., 2015). Investigators do not need to know people's names to gather rich profiles (Saunders, Kitzinger, & Kitzinger, 2014).

Qualitative researchers face new challenges to maintain confidentiality of previously classified private data now readily available on the Internet. Study participants completed and returned the consent forms prior to the interviews. Subsequently, I assigned the following codes to keep the study participants' names confidential (a) CS-1 for the first participant, (b) CS-2 for the second participant, (c) CS-3 for the third participant, and (d) CS-4 for the fourth participant.

Data Retention Protection Plan

The plan for data retention contained the following requirements (a) password protect electronic research files, (b) electronically store project data, (c) file paper notes

and research documents in a locked file cabinet, (d) store electronic data on a password protected encrypted backup disk drive, (e) retain data files in my home in a locked file cabinet for 5 years following the conclusion of the multicase study (NIH, 2012), and (f) shred and destroy data at the end of the 5 year retention period. Additionally, per NIH (2012) guidelines, I protected the participants' rights throughout the project's lifecycle.

Data Collection Instruments

Data collection is a phased series of events generating significant amounts of data from multiple resources to fit diverse experiences into predetermined response categories (Baškarada, 2014; Gale et al., 2013; Morse & McEvoy, 2014). The data collection plan utilized a purposive snowball sampling strategy on four SME owners in the retail business located within a 5-mile geographic area in Melbourne, Brevard County, Florida, within zip codes 32901 and 32903, exploring decisions regarding successful SME cyber security strategies and practices. The review of relevant company documents is a strategy, which increases data reliability and rigor (Baškarada, 2014; Cronin, 2014; Gale et al., 2013). During the initial phase of the collection process, I (a) obtained and analyzed relevant company documents, e.g., business, training, security, risk management, or contingency plans; (b) conducted and digitally recorded the face-to-face semistructured interviews with the selected SME owners; and (c) to ensure data saturation, interviewed participants until no new data or knowledge emerged.

The most valid form of qualitative data collection is personal interviews since they capture human interactions and emotions (Marshall & Rossman, 2016; Morse & McEvoy, 2014; Pacho, 2015; Yin, 2014). Appendix A contains the interview questions,

Appendix B is the participant recruitment letter, and Appendix C outlines the interview protocol. For the study, SME owner participation was through a purposive snowball sampling. Collecting data is an essential element within any research study and may consist of many phases.

The first phase of the data collection process consisted of a review of relevant company documents where I was the primary data collection instrument for the multicase study of four SME owners. After obtaining and examining documents, such as business, training, security, risk management, or contingency plans, identification of the key components of general cyber security strategies and practices developed and best practice themes emerged. Moreover, document reviews provided additional insight about SME owners' effective cyber security strategies and preventative measures.

The preferred method of conducting face-to-face semistructured interviews is in natural settings to capture rich, descriptive human experiences enabling official participant responses. Telephone and e-mail interviewing techniques are also valid; however, these methods do not capture human interaction. Technology advances on the Internet have greatly improved qualitative online interviewing inquiry and have virtually eliminated the concurrent, collaborative interaction related to face-to-face interviews (Janghorban et al., 2014).

The second phase of the data collection process consisted of conducting semistructured interviews in person at the agreed upon locations using the SME Owner's Cyber Security Strategies Interview Questions (see Appendix A) to explore participants' experiences related to cyber security practices. Prior to the beginning of the interview,

each participant acknowledged and provided affirmation to digitally audio record the interview. Additionally, at the beginning of each recorded interview and prior to the first interview question, each participant affirmed informed consent. After each interview, participants asked questions, and provided additional data.

Member checking is an important component of validation in qualitative research to determine if the researcher accurately reported the participants' statements (Harvey, 2015; Koelsch, 2013; Palinkas, 2014). Likewise, member checking validates interview interpretations and increases data reliability (Cleary et al., 2014; Fusch & Ness, 2015; Houghton et al., 2013). Moreover, the use of member checking ensures the captured meaning as well as word choice (Elo et al., 2014; Houghton et al., 2013; Pacho, 2015; Yin, 2014). Elo et al. (2014) reported technological advancements in automated methods provide researchers faster and more accurate means to translate, code, and analyze collected data. Member checking, triangulation, and peer debriefing promote trustworthiness in qualitative studies (Koelsch, 2013; Nottingham & Henning, 2014; Palinkas, 2014).

To maximize data reliability and validity, I transcribed and interpreted each interview, provided participants the transcription of their individual data interpretation files for member checking, and requested comments on accuracy. Participants received an e-mail with a copy of their data interpretation file for member checking review and a request for return comments/concurrence within 2 days. Participants understood if they failed to respond within the specified timeframe, they agreed with the accuracy of the data interpretation file. If a respondent provided comments, within 1 day a revised data

interpretation file was available for review via e-mail for additional feedback and concurrence. If the participant provided no further comments within 2 days, the participant understood he/she provided concurrence. Following the member checking phase, the data interpretation files were imported into a database to categorize, code, and theme the collected data from the review of relevant company documents and data interpretation files for additional analysis.

Data Collection Technique

Researchers have used multiple data collection techniques, such as document reviews, archival record reviews, physical artifacts, observations, interviews, and reflective journals, to gather qualitative data (Onwuegbuzie & Byers, 2014; Pacho, 2015; Sangster-Gormley, 2013; Yin, 2014). Additionally, research experts cited utilizing multiple data sources increased data reliability and significant substantiation of emerging data (Marshall & Rossman, 2016; Morse & McEvoy, 2014; Pacho, 2015; Patton, 2015; Yin, 2014). I reviewed relevant company documents and conducted participant interviews.

An evaluation of supplementary company documents and external resources provides another data collection mechanism to capture qualitative case study research (Baškarada, 2014; Marshall & Rossman, 2016; Pacho, 2015; Patton, 2015; Yin, 2014). Researchers suggested to maximize interview depth, investigators use multiple sources of evidence consisting of document reviews and personal interviews (Marshall & Rossman, 2016; Morse & McEvoy, 2014; Pacho, 2015; Yin, 2014). Moreover, Yin (2014), Patton (2015), and C. Marshall and Rossman (2016) recommended a review of relevant

company documents, such as company magazines, policies, procedures, or sustainability reports before conducting interviews. Using a consistent data protocol enhances cross case analysis in qualitative research (Baškarada, 2014; Elo et al., 2014; Yin, 2014).

Case study research thick description involves capturing the rich details of the case and figuring out the complex layers of understanding the structure of the social domain (Baškarada, 2014; Elo et al., 2014; Pacho, 2015). Adequate contextual description is required to understand the case setting (Hyett et al., 2014). I used multiple sources of evidence and depicted the environmental setting using rich descriptions.

Semistructured interviews consisting of open-ended questions provide both the interviewer and interviewees opportunities to elaborate on the phenomena topic (Marshall & Rossman, 2016; Morse & McEvoy, 2014; Yin, 2014). The second part of the data collection for the qualitative multicase study project consisted of four interview sessions using a standardized set of eight questions to explore and investigate the SME owners' experiences related to cyber security strategies. Interview protocols contain not only research questions, but guide the researcher through the entire interview process (Marshall & Rossman, 2016; Pacho, 2015; Patton, 2015; Yin, 2014).

Appendix D contains the interview protocol to ensure the interviewer asked each participant the same questions in the same sequence during each interview. I conducted semistructured interviews in person at the agreed upon locations using the SME Owner's Cyber Security Strategies Interview Questions (see Appendix A) to explore participants' experiences related to cyber security practices. After each interview, I gave the participant an opportunity to ask questions, or provide additional data.

The concept measured by the instrument was to understand cyber security phenomena and identify potential preventative measures, which may apply to a larger sample population. Collection of participant data was through face-to-face semistructured interviews in natural settings. The interview approach was a collaborative partnership between the interviewer and the participants, guiding the conversation with the participants and then encouraging participants to expand responses to capture rich descriptions. Prompting the participants may generate more in-depth descriptions of experiences yielding a richer descriptive analysis report (Baškarada, 2014; Elo et al., 2014; Marshall & Rossman, 2016; Yin, 2014). During semistructured interviews, participants discussed what factors influenced decisions about cyber security practices. I interpreted each digitally recorded file into a textual format to validate raw data.

The framework method, which sits within a comprehensive family of examination approaches described as thematic analysis, has been a popular approach to managing and analyzing data in multidisciplinary research (Baškarada, 2014; Gale et al., 2013; Patton, 2015; Yin, 2014). Researchers stressed the importance of documenting field notes from interviews after each interview (Cronin, 2014; Pacho, 2015; Patton, 2015). The first phase of data analysis consisted of reading the data transcription twice to verify the accuracy of the digital recording interpretation against the original voice recording.

Member checking is a critical component of trustworthiness and assists with data interpretation and validation (Harvey, 2015; Koelsch, 2013; Nottingham & Henning, 2014). To maximize data reliability and validity, I provided all participants the transcription of their data interpretation files for member checking and requested

comments on accuracy. After the interview cycle, I categorized, coded, and themed the data collected from an examination of relevant company documents and participant interviews for further analysis.

There are advantages and disadvantages to each data collection technique. Document reviews are advantageous to research since they are unobtrusive and inexpensive, provide robust background information, and may highlight issues not discovered by other data collection means (Sangster-Gormley, 2013; Wolfswinkel, Furtmueller, & Wilderom, 2013; Yin, 2013). A primary disadvantage of document reviews is the time to collect, review, and analyze vast amounts of data, which may be incomplete or not be available within the required research study period (Owen, 2014; Pacho, 2015; Wolfswinkel et al., 2013). Interviews provide a benefit by prompting the participants to elaborate and describe what is most important to them (Pacho, 2015; Patton, 2015; Robinson, 2014). A primary disadvantage in using interviews is interview bias (Elo et al., 2014; Pacho, 2015; Robinson, 2014; Yin, 2014).

Data Organization Technique

The most common data collection methods used in qualitative research incorporate interviews, observations, and document review (Pacho, 2015; Yilmaz, 2013; Yin, 2014). Three critical components when performing qualitative research include selecting the participants, performing data analysis, and ensuring research quality and rigor (Baškarada, 2014; Elo et al., 2014; Marshall & Rossman, 2016; Paulus, Woods, Atkins, & Macklin, 2017; Yin, 2014). Managing the vast amounts of data can be an overwhelming task.

The most important decision when conducting structured qualitative research is choosing the right software program, which increases research rigor (Sotiriadou, Brouwers, & Le, 2014; Yin, 2014). An element to consider when selecting the best tool is the ease in which the researcher can integrate information across many different functions and purposes while conducting qualitative research. A multicase study database allows investigators to develop an audit trail from various phases, such as data collection, analysis, reflectivity, and conclusions (Baškarada, 2014; Elo et al., 2014; Yin, 2014). The NVivo project file provides an audit trail for this research study. Table 1 shows a sample code list for the reflective journal and research log.

Table 1

Sample Code for Reflective Journal and Research Log

Element	Reflective Journal	Research Log
SME owners' executing secure business operations	X	
SME owners' knowledge of cyber security	X	
SME owners' risk assessment decision making	X	
Selecting participants		X
Obtaining archival company documentation		X
Conducting face-to-face interviews		X

NVivo is a commercially licensed software suite assisting users in organizing, analyzing, and sharing collected data from interviews, observations, focus groups, and

literature reviews (Castleberry, 2014; Houghton et al., 2015; Paulus et al., 2017). The NVivo software application is a user-friendly tool, which enables users to create projects and organize collected research data according to type (Castleberry, 2014; Houghton et al., 2015; Zamawe, 2015). NVivo supports the management and synthesis of qualitative research enabling the researcher to retrieve data quickly and sort, categorize, browse, code, and interpret the data records. Users create projects containing data sets based on interviewee and further subcategorize data based on user-defined parameters. NVivo assists researchers with organizing, classifying, and analyzing nonnumerical data in an electronic versus manual method (Houghton et al., 2013; Sotiriadou et al., 2014; Zamawe, 2015). Using the NVivo software application to analyze data has little or no influence on the design of the research (Zamawe, 2015).

I imported the doctoral research study files consisting of data collected from an examination of relevant company documents, and semistructured recorded interviews of four SME owners in Melbourne, Brevard County, Florida, into the NVivo software application. Additionally, the database contained multiple formats including raw audio recorded data, interview interpretation files, member checked files, and field notes to allow complex data analysis. Researchers are required to securely maintain and store all raw data (NIH, 2012). Consequently, I will maintain and store all raw data in my home in a locked file cabinet for 5 years after the study concludes.

Data Analysis

The data analysis for the research study included an examination of documents, audio and digital recording, member review comments, word processing entries, database

development, structured queries, and narrative descriptions. The research database consisted of data from examination of relevant company documents, and semistructured recorded interviews of four SME owners in Melbourne, Brevard County, Florida. Additionally, the database contained multiple formats including raw audio recorded data, data interpretation files, member checked files, and field notes to facilitate complex data analysis.

The NVivo software provides features to automate and analyze data generated from selected inputs. Utilizing the NVivo software, I performed complex data analysis by creating multiple data sets, while maintaining the original data set, for trends pertaining to SME owners' cyber security practices. Analyzed results provided data about the participants' cyber security practices and factors influencing decisions. In qualitative data analysis, ensuring reliability and validity is important throughout the research project (Baškarada, 2014; Palinkas, 2014; Sotiriadou et al., 2014).

According to Houghton et al. (2015), there are no systematic rules for analyzing qualitative data. Researchers have many different methods to analyze qualitative data; however, the most commonly used method is thematic analysis (Gale et al., 2013; Houghton et al., 2015; Marshall et al., 2013). I assessed the cyber security strategies of small retail business owners with annual gross revenues of less than \$10 million by using thematic analysis. The first data source to explore the case study was an examination of relevant company documents; the second and primary data source was through semistructured interviews.

The data analysis process logically and sequentially addressed the research question by utilizing analysis techniques designed for qualitative studies. The first step was to back up research data recorded on the computer hard drive to both a thumb drive and an external hard drive. The next step was to read the transcribed data multiple times to analyze and uncover specific patterns and themes.

The framework approach is a suitable form for analyzing text and interview data by using a systematic and logical method to identify similarities and differences in a qualitative data set (Gale et al., 2013). The framework approach enables the researcher to view data, compare and contrast data sets, and identify relationships by using thematic analysis while maintaining the individual's original data record intact. My conceptual framework strategy leveraged the systems theory framework. Additionally, the NIST framework provides common standards, guidelines, and practices for SME owners which highlights the basics of cyber security and information security, including defining the type of information, which needs protection, some of the common cyber threats, and informs users of known cyber security best practices (NIST, 2015b; Schneck, 2014).

Following analysis of the semistructured interviews and transcriptions, patterns and themes emerged from the data. The development of themes involves a systematic search for patterns generating interpretive concepts, which describe or explain the data (Baškarada, 2014; Gale et al., 2013; Houghton et al., 2015). Research coding is an iterative and phased process performed at different levels of abstraction (Baškarada, 2014; Gale et al., 2013; Houghton et al., 2015). Confidentiality, integrity, and access (CIA) are critical elements for information security processes SME owners implement

(SBA, 2015). CIA themes emerged from the examination of documents, interviews, journal entries, and field notes.

Researchers provided helpful guidance to new researchers to read the collected data multiple times to identify keywords and phrases (Paulus et al., 2017; Vaismoradi, Turunen, & Bondas, 2013; Zamawe, 2015). First, I manually identified keywords and phrases by methodically reviewing relevant company documents and each interview transcript multiple times to determine keywords and phrases; then used the NVivo application to identify keywords using its analytical software specifically designed to identify words and phrases and compared the two data sets. Coding highlighted significant statements, quotes, or sentences further providing an understanding of the participants' responses.

Cleary et al. (2014), Gale et al. (2013), and Paulus et al. (2017), emphasized categorization of data into distinct groupings. The researcher used NVivo to categorize coded data by type and sub-type, always keeping the original data set intact. Finally, I conducted multiple data analyses which determined relationships and trends indicated in Section 3 of the doctoral study.

Researchers emphasized using multiple sources of evidence to collect data for case study research: documents, archival records, physical artifacts, interviews, direct and participant observations (Baškarada, 2014; Marshall et al., 2013; Yin, 2014). I used multiple sources of evidence to strengthen the case study and developed a database to collect and organize archival materials and notes. Additionally, the researcher utilized

NVivo to maintain the chain of evidence to increase the quality and reliability of the study research.

Fusch and Ness (2015) described triangulation as a method for qualitative researchers to explore different levels and perspectives of the same phenomenon thereby enabling researchers to check and establish the validity of the study's results.

Researchers suggested utilizing one of the triangulation methodologies, such as data, investigator, theory, or methodological to support data saturation and validity (Carter, Bryant-Lukosius, DiCenso, Blythe, & Neville, 2014; Fusch & Ness, 2015; Patton, 2015; Yin, 2014). During the data analysis phase, methodological triangulation ensures data saturation and is an appropriate technique to correlate data from multiple data collection sources for the multicase study (Carter et al., 2014; Castleberry, 2014; Fusch & Ness, 2015; Paulus et al., 2017).

Compliance with methodological triangulation occurs by employing multiple data sources, such as interview analysis, creation, and utilization of an NVivo database, and providing an audit trail documenting the integrity of data from inception to completion (Castleberry, 2014; Paulus et al., 2017; Yilmaz, 2013). I utilized methodological triangulation and maintained a case study database populated with the raw, sorted, themed, and interpretive data. Additionally, the researcher will store the digitally encrypted data for the study, which consists of field notes, data recordings, participant member reviews, e-mails, and interpretative data files, in a locked file cabinet in her home for 5 years after the study concludes.

Codes Developed for Interview

The primary purpose of grouping and coding the research interview questions was to provide a list of codes for data developed from participant interviews. The secondary purpose was to explain the processes for developing the coding themes from the semistructured interview. Appendix A shows the interview questions.

Qualitative research consists of collecting data from responses to open-ended questions sometimes yielding the data results as indistinct and unstructured (Aaltonen & Tempini, 2014). By reviewing, categorizing, and interpreting the data, the interrelated analysis phases assist in interpreting the data using multiuse categories (Elo et al., 2014; Marshall & Rossman, 2016; Paulus et al., 2017; Yin, 2014). Critical elements contained in these phases included organizing and preparing collected data for analysis, thoroughly reading the collected data material, segmenting the data using defined coding methodology, coding the collected data into categories, highlighting data in defined colors for each category, developing theme representations, and finally, interpreting the data.

Development of Coding System

Developing a coding system involved thoroughly reading the collected data. After analyzation, the researcher used keywords to index and sort data into similar categories, themed, and divided data into manageable sections of information. Researchers recommended entering the data into a software application designed to find patterns and trends to assist in understanding the data (Gale et al., 2013; Marshall & Rossman, 2016; Paulus et al., 2017). After review of the data analysis, similarities and

variances emerged. These patterns, trends, and variances assist in providing predictive metrics to forecast similar events (Fletcher, Massis, & Nordqvist, 2016; Gale et al., 2013; Yin, 2014). Table 2 shows codes and meanings used to categorize similarities and trends, which emerged during data collection. Strategies subcategories included protect, information technology, security, risk management, and employee training.

Table 2

Coding Legend

Code	Meaning
Strategies	Has cyber attack plan
Impacts	Understands financial implications if breach occurs
Policy	Has adequate current cyber security policies
Prevention	Has business strategy to prevent cyber security attacks
Third-party	Has defined business strategy to protect company data
Training	Values employee training

Interview Coding Summary

Detecting similarities among respondents' answers provides a method of correlating data thus revealing patterns and trends (Elo et al., 2014; Fletcher et al., 2016; Gale et al., 2013; Marshall & Rossman, 2016). Researchers often utilize matching patterns to create themes (Fletcher et al., 2016; Gale et al., 2013; Marshall & Rossman, 2016; Yin, 2014). I used coded and themed data to identify patterns for data analysis to find patterns and trends.

Data Analysis Summary and Presentation

Frameworks are the logical structure for shaping research studies and are dependent on the type of selected research method (Fletcher et al., 2016; Onwuegbuzie & Byers, 2014; Yin, 2014). The qualitative multicase study research focused on a conceptual framework leveraging the systems theory to explore what effective cyber security strategies SME owners utilized to deter cyber attacks. The data presentation for the doctoral study consisted of written analysis supplemented with a table and figures depicting trends and patterns on collected data.

Reliability and Validity

In qualitative research, establishing trustworthiness of the data assesses the reliability and validity (Baškarada, 2014; Elo et al., 2014; Marshall & Rossman, 2016). Yin (2014) reported taking precautions during the design of a study and preparation for how applicable the findings will be to a larger population enhanced measurement of reliability and validity. The trustworthiness of qualitative studies consists of credibility, dependability, confirmability, and transferability (Elo et al., 2014; Houghton et al., 2013; Noble & Smith, 2015; Wahyuni, 2012).

Reliability

Research reliability refers to the extent in which research findings are producible in an accurate and ethical manner, replicable, and transferable to a larger population (Baškarada, 2014; Houghton et al., 2013; Tong et al., 2013). Member checking is a critical component of validation in qualitative research to determine if the researcher accurately reported the participants' statements (Harvey, 2015; Koelsch, 2013; Palinkas,

2014; Valizadeh, Dadkhah, Mohammadi, & Hassankhani, 2014). Furthermore, member checking corroborates interview interpretations, ensures the captured meaning as well as word choice, and increases data reliability (Cleary et al., 2014; Elo et al., 2014; Fusch & Ness, 2015; Houghton et al., 2013). To enhance the dependability of the qualitative multicase study, I (a) used multiple data collection sources, including the review of relevant archival documents and conducting semistructured interviews; (b) administered all interviews using the interview protocol; (c) utilized member checking; and (d) consistently examined items such as raw data, field notes, and data products to verify data.

Establishing research quality requires ensuring mutual reliability and legitimacy of investigation findings. The trustworthiness of a research study is essential in determining its merit (Baškarada, 2014; Elo et al., 2014; Houghton et al., 2013). The research study consisted of face-to-face semistructured interviews with four SME owners in Melbourne, Brevard County, Florida.

The targeted population consisted of SME owners in the retail business located in Melbourne, Florida, within the zip codes of 32901 and 32903 employing less than 250 employees and having annual gross revenues of less than \$10 million, who utilized the Internet for business operations and had successfully implemented cyber security strategies. Following NCSA (2015) and “Protecting Small Businesses Against Emerging and Complex Cyber-Attacks” (2013), the selected population in this study was appropriate because among SME owners who suffered a cyber attack, 60% went out of business within 6 months after the first cyber attack.

Validity

Researchers enhance the validity of their research findings through verification and validation of data. Credibility is a critical element for the internal qualitative data validation process and consists of establishing believable research findings from the research participants' perspective (Carter et al., 2014; Elo et al., 2014; Noble & Smith, 2015). A study is credible when reviewers outside the study recognize the findings, and they can be applied to other groups or settings (Noble & Smith, 2015; Petty, Thomson, & Stew, 2012; Wahyuni, 2012).

For the study, I first conducted an examination of relevant company documents. Next, I conducted face-to-face semistructured interviews using an established interview protocol (see Appendix D) to collect data. Data validation and verification for the qualitative research study uses respondent corroboration through participant member checking (Valizadeh et al., 2014). Member checking promotes trustworthiness in qualitative research, captures different dimensions of the same phenomenon, and increases credibility (Houghton et al., 2013; Nottingham & Henning, 2014; Valizadeh et al., 2014).

Cross verifying data incorporates triangulation, member checking, and analysing sets of data using NVivo software queries (Castleberry, 2014; Houghton et al., 2013, 2015). Further data analysis using keyword assimilation predicts patterns and trends potentially yielding similarities in responses. Utilizing multiple data resources and maintaining an audit trail of decisions made during the research process increases credibility (Houghton et al., 2013; Marshall & Rossman, 2016; Pacho, 2015; Yin, 2013).

Review of multiple lines of evidence, theories, and methodologies throughout the study strengthened the research and addressed research validity.

Transferability refers to the applicability of project findings to a similar group or generalized population (Elo et al., 2014; Petty et al., 2012; Wahyuni, 2012). Rich and thick descriptions enable the readers to decide on their own if the research results are transferable to their context (Onwuegbuzie & Byers, 2014). Researchers recommend analyzing data from multiple sources, using various methods, and maintaining an audit trail of decisions made during the research process to increase credibility (Elo et al., 2014; Houghton et al., 2013; Wahyuni, 2012).

Methodological triangulation of multiple sources will be a contributing factor for the study's transferability (Baškarada, 2014; Elo et al., 2014; Fusch & Ness, 2015; Heale & Forbes, 2013). Data source and method types strengthen the validity of a case study evaluation (Yin, 2013). A case study protocol contributes to the reliability by standardizing the investigation (Baškarada, 2014; Marshall & Rossman, 2016; Yin, 2014).

Two strategies for reassuring reliability in the exploratory case study included the case study protocol and case study database. To ensure transferability and applicability to other situations, thick descriptions of the participant data, raw examples of data, along with demographics and geographic limitations will assist with subsequent research initiatives (Houghton et al., 2013; Palinkas, 2014; Wahyuni, 2012). I employed methodological triangulation and maintained a case study database populated with the raw, sorted, themed, and interpretive data.

Carter et al. (2014) reported triangulation is a qualitative research strategy used to test validity through the convergence of information from different sources.

Confirmability throughout the data collection process signifies the extent to which others confirm or corroborate research results (Baškarada, 2014; Elo et al., 2014; Wahyuni, 2012). Developing an audit trail is a technique to foster confirmability (Baškarada, 2014; Wahyuni, 2012; Yin, 2014).

A second technique to achieve confirmability is through reflexivity (Mayoh & Onwuegbuzie, 2015; Onwuegbuzie & Byers, 2014). Field notes, transcripts, and audio recordings are acceptable means of qualitative data collection (Cronin, 2014; Houghton et al., 2013; Smith & Noble, 2014). To ensure confirmability, I created a data collection database to maintain an audit trail depicting the decisions during the research process including field notes, memos, and reflexivity journal entries; employed member checking; utilized methodological triangulation; mitigated personal bias, and reported results findings in an honest and ethical manner.

Elo et al. (2014) stressed the importance of obtaining the optimal sample size for qualitative research, which depends on the purpose of the study, research questions, and richness of the data. Data saturation is through a series of data collection events generating large amounts of data from multiple resources, which fit diverse experiences into predetermined response categories (Morse & McEvoy, 2014). Saturation exists when no new data, concepts, or themes occur in subsequent interviews causing an interview redundancy (Boddy, 2016; Cleary et al., 2014; Elo et al., 2014).

Several factors determine saturation and small studies may achieve saturation quicker than large studies; controlling the size and scope of the case study assists with data saturation (Boddy, 2016; Fusch & Fusch, 2015; Smith & Noble, 2014). To ensure data saturation in the study, I interviewed participants until no new data or knowledge emerged. Redundancy and lack of any new concepts or emerging knowledge from collected data confirm data saturation (Houghton et al., 2013; Marshall et al., 2013; O'Reilly & Parker, 2013).

The data collection plan utilized a purposive snowball sampling methodology on four SME owners in Melbourne, Brevard County, Florida, to explore their cyber security strategies and decisions regarding preventative cyber security practices. The collection process required examination of relevant company documents, and conducting and digitally recording, face-to-face semistructured interviews with four participants. Data evidence gathering is dependent on the redundancy of material and ceases when no new data emerges (Cleary et al., 2014; Fusch & Ness, 2015; O'Reilly & Parker, 2013; Smith & Noble, 2014). The research study used a consistent combination of techniques for comparing and crosschecking data, which increased reliability and validity of the study and compensated for any weakness found in a single data approach.

Transition and Summary

The pervasiveness of cyber attacks and increased criminal activities affecting businesses is a new societal phenomenon requiring further exploration in preventative solutions. Theft of sensitive information can be an expensive loss to SME owners. The qualitative case study provided SME owners' perceptions of cyber security practices,

behaviors, and awareness about cyber attacks. The data from the study might make a social impact on SME owners by increasing their knowledge of cyber security methodologies, providing sustainable cyber security strategies to alleviate or mitigate future cyber attacks, and enhancing their potential for success.

Section 2 contained a review of the research purpose and problem, justified the selected research method and design, included data collection instruments, and participant and sampling methodologies. Additionally, Section 2 described the analysis strategy and tools and explained techniques for ensuring an ethical, reliable, and valid research study. Case study methodology best supports the qualitative research by answering the *how* and *why* of phenomena by interpreting the open-ended, narrative findings. The data collection plan for the multicase study utilized the purposive snowball sampling methodology on four SME owners in Melbourne, Brevard County, Florida, to explore their effective cyber security strategies and decisions regarding preventative cyber security practices. Semistructured interviews consisted of open-ended questions providing the interviewees the opportunity to elaborate on effective SME cyber security strategies. Employing NVivo qualitative software analysis techniques allowed classification and analyzation of nonnumerical research data.

Section 3 includes an overview of the qualitative study, presentation of conclusions based on the collected research data and analyzed results, application of the study to professional business practices, and potential implications for social change. Additionally, I provided recommendations for modification of cyber security business practices for SME owners based on analysis through examination of documents and from

semistructured, face-to-face, digitally recorded interviews. Lastly, recommendations for action, recommendations for further research, my reflections and experience within the process, and the DBA Doctoral Study's conclusion complete section three.

Section 3: Application to Professional Practice and Implications for Change

Introduction

The purpose of the qualitative multicase study was to explore effective strategies SME owners use to protect their businesses from cyber attacks. The specific population consisted of four owners of SME businesses in the retail industry who (a) utilized the Internet for business operations; (b) were licensed to operate a retail business in the metropolitan area of Melbourne, Brevard County, Florida; (c) employed between 1-249 personnel; (d) had an annual gross revenue of under \$10 million; and (e) had successfully implemented cyber security strategies. The conceptual framework for this study was the GST. Archival company documentation and participant interview responses provided the data I used to address the research question. Three major themes emerged: (a) cyber security strategy, (b) reliance on third-party vendors for infrastructure services, and (c) cyber security awareness. My analysis of the research study findings indicated the effective strategies successful SME owners use to protect their businesses from cyber attacks.

Presentation of the Findings

The central research question for the study was: What effective strategies do SME owners use to protect their businesses from cyber attacks? I used review of archival documents and semistructured interviews with open-ended questions (Appendix C) to collect data for the study; however, I collected the largest amount of data from participant interviews. I achieved data saturation when the interview respondent data and archival company documents I reviewed became repetitive, and no new information materialized.

As the primary research data collection instrument, I created a database and maintained an audit trail of study participant correspondence, journal notes, and archival documentation. I analyzed the research study data using QSR International NVivo by importing archival company documentation, participants' answers to the interview questions, the member-checked interpretative files, and interview notes.

The document and archival analysis of SME owners' documents, which included business reports and company policies, provided corroborative support to the participant interviews and enabled triangulation in the data collection process. Pseudonyms I used for participants in the study were SME Owner 1 (CS-1), SME Owner 2 (CS-2), SME Owner 3 (CS-3), and SME Owner 4 (CS-4). Three major themes emerged from the triangulated data analysis, based on the frequencies of coded node responses: (a) cyber security strategy, (b) reliance on third-party vendors for infrastructure services, and (c) cyber security awareness. Figure 1 shows the emergent themes for effective strategies SME owners use to protect their businesses from cyber attacks.

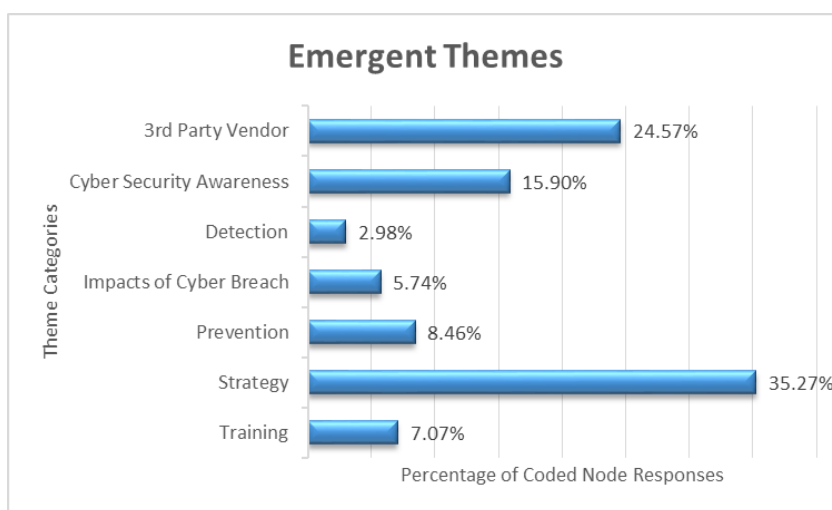


Figure 1. Emergent themes of SME owners' effective cyber security strategies.

The data collection and analysis provided me a basis for understanding effective cyber security strategies SME owners use to protect their businesses from cyber attacks. Using the NVivo data analysis software, I categorized and thematized relationships obtained from archival company documents and the interviews. I ensured that I had achieved data saturation by using methodological triangulation and member checking.

The findings of the research study aligned well with the systems theory in that each emergent theme is dependent upon the other. Von Bertalanffy (1968) developed systems theory, which he characterized as the study of interrelationships rather than individual modules. Von Bertalanffy contended that systems, in essence, are self-regulating and self-correcting. SMEs are systems consisting of different components, one of which is information security (Gomes, 2015). Atoum and Otoom (2016) emphasized the importance of cyber security for SME owners as a critical systems component. Rather than SME owners utilizing each theme independently, they can leverage them by using them together for more efficient sustainable business operations. Similarly, Shin and Konrad (2017) claimed that von Bertalanffy's GST enables organizations to meet their objectives, and declared that organizations that incrementally adapt human resource management practices create a competitive advantage.

The first theme, cyber security strategy, was reflected by the predominant coding node *security plan* during the data analysis. The second theme, reliance on a third-party vendor for infrastructure services and cyber security prevention, emerged following data analysis and was reflected by the predominant coding node *secure provider*. The third

emergent theme, cyber security awareness, was evidenced by the predominant coding node *prevention* during the analysis of archival and interview data.

During data analysis, some keywords such as training, strategy, and third-party vendor emerged in more than one theme. The research study results showed the GST of concept of *interconnectivity* in the duplication of keywords in emergent themes and subthemes. Each theme is connected and continuously evolving based on global events and business needs. The significance of exploring SME owners' successful implementation of cyber security best practices, is that my findings may mitigate data breaches and prevent cyber attacks. According to the U.S. GAO (2013, 2015), pervasive and sustained cyber attacks might have a potentially devastating impact and could disrupt the operations of individuals, businesses, and governments.

Theme 1: Cyber Security Strategy

The first major theme to emerge during data analysis of archival documents and participant interviews was the use of cyber security policy and implementation of procedures to protect, defend, and react to cyber attacks. My analysis indicated the requirement for SME owners to establish cyber security policies and effectively implement cyber security procedures to protect their businesses from cyber attacks. Sheppard et al. (2013) reported both public and private organizations require a robust cyber security strategic approach to prepare, respond, and recover from cyber attacks.

SME owners must take a proactive approach to protect their data by establishing cyber security plans, and creating and implementing Internet security policies (DHS, 2015b; SBA, 2014). Research participants showed resilience in adapting to a changing

environment by implementing effective cyber security strategies. Figure 2 shows data analysis results of archival documents and SME participant responses for subthemes relevant to cyber security preventative measures.

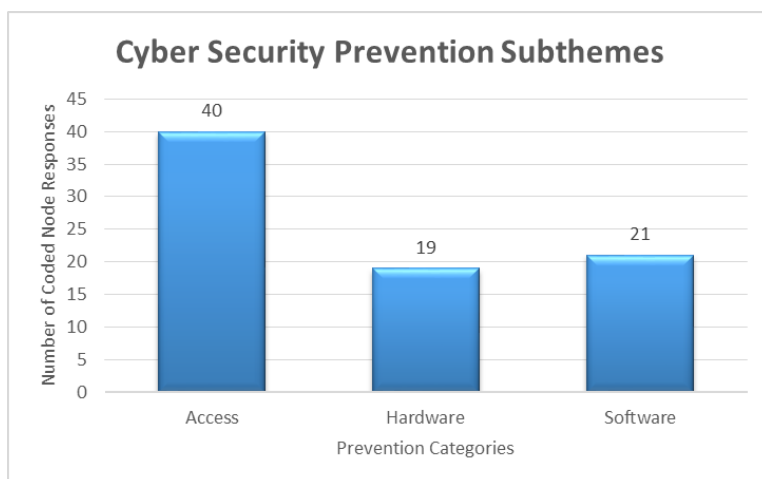


Figure 2. SME owners' cyber security prevention subthemes.

According to Shackelford et al. (2015), 80% of small business owners do not have established cyber security policies. Conversely, the information I obtained in this research study provided new data that shows the strategies of SME owners who have implemented cyber security policies. These and other SME owners are implementing effective preventative actions to protect their businesses from cyber attacks. The successful strategic plans included (a) limiting system access through password protection methods, (b) establishing a cyber security plan, (c) ensuring cyber security awareness, (d) conducting training, and (e) implementing security procedures. Figure 3 shows data analysis of archival data and participant responses, by showing the highest number of coded node responses of SME owners' successful cyber security strategy subthemes.

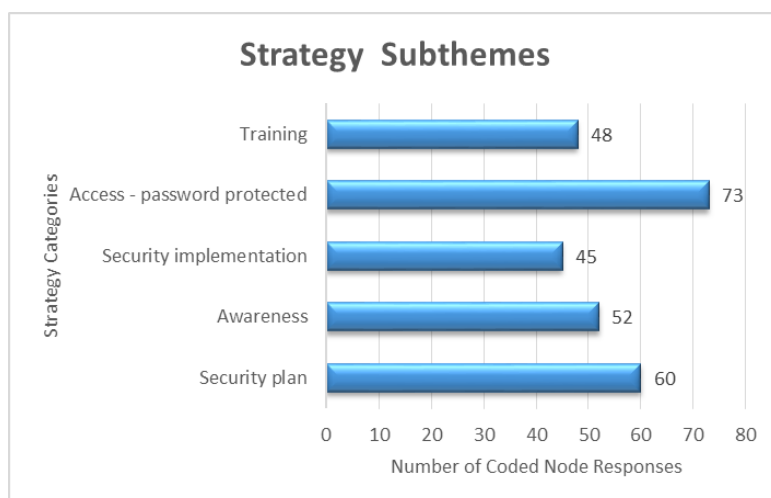


Figure 3. SME owners' successful cyber security strategy subthemes.

Limiting access by password protection. To prevent financial loss resulting from network hacking and security breaching by users whose sole purpose is to gain access based on a user's or system's weakness, companies should invest in securing their data (DHS, 2015a; FBI, 2015c). My analysis of archival documents and interview responses indicated SME owners ensure explicit awareness and compliance with their established security and privacy policies. Analysis of Participant CS-1 and CS-2's security plans indicated access to business systems, "required logins and unique passwords." Participant CS-3's written security policy contains the requirement for unique logins and passwords to "protect against the unauthorized access, use, alteration, or destruction of potentially personally identifying information." Review of written privacy policy for Participant CS-4 showed the requirement for unique logins and passwords, and that "clients are responsible for maintaining the confidentiality of account information and passwords." Business owners' first line of defense to preventing data loss is to implement valid user passwords (Cheswick, 2013).

My analysis of archival documents and interview responses from the study participants showed each SME owner imposes basic cyber security preventative measures by requiring user logins and passwords to access business systems. Participants CS-2, CS-3, and CS-4 require a unique login and valid password to access business systems. Additionally, Participant CS-1 requires a unique password and login, or for faster access, employees can opt to use fingerprint scans to access business systems. Table 3 shows the various approaches SME owners use to limit access to business systems.

Table 3

Cyber Security Measures to Limit Access

Access Method	Participant CS-1	Participant CS-2	Participant CS-3	Participant CS-4
Unique Login	X	X	X	X
Unique Password	X	X	X	X
Fingerprint Scan	X			

According to the SBA (2014), loss of data affects businesses and has the potential to jeopardize a company's reputation with customers, suppliers, and partners. SME owners' knowledge of preventative actions highlighted access, hardware, and software as the primary data subthemes to counter cyber threats. Employee and customer access are the biggest data drivers, followed by software operating system patches and virus protection, and hardware firewall and router encryption. Analysis of archival security plan documents and interview responses revealed password protection was the primary

data node for the access category. All participants enforce password protection to gain access to business systems. Participant CS-1 stated,

Inside the business operations, we utilize employee logins with either a password or a fingerprint scan. The fingerprint scan recognition feature provided by our third-party vendor is an extra charge to the business; however, when employees use it, the results are very easy and fast.

Participant CS-3 affirmed, “Both employees and customers must use a password to gain access to our application we use for business.” Additionally, Participant CS-4 reiterated, “Our business and customers may access our website system using a unique login and password from a computer, tablet, or mobile device.” Participant CS-2 stated, “I do not provide customer access to any of the business systems.” In addition, Participant CS-2 responded, “I limit employee Internet access to approved websites only. All other websites require permission.”

Global wired and wireless technology improvements provide businesses enormous benefits yet simultaneously expose companies to potential vulnerabilities (Weber & Horn, 2017). The creation of wireless systems technology provides another vulnerability to tracking and reporting (Denning et al., 2013). My analysis of archival documents and participant interviews indicated Participants CS-1, CS-3, and CS-4 shared a common theme by providing Wi-Fi access to the Internet to both their employees and customers using a unique password, while Participant CS-2 did not provide Wi-Fi access to the employees or customers. When probing further on why Participant CS-2 elected

not to provide Wi-Fi access, Participant CS-2 stated, “Most people now have smart phones, and they access the Internet via their own devices using their own plan.”

Cyber security plan or process. Emm (2013) addressed six security steps, which SME owners can employ to protect themselves (a) require user passwords for login accounts, (b) select products which provide protection, (c) protect and secure systems data, (d) establish and implement user policies and procedures, (e) properly train staff to recognize and understand the risks, and (f) expect and prepare for the worst.

Participant CS-3 described a three-step process used to prevent and detect cyber attacks:

The first step is prevention by utilizing a third-party vendor’s infrastructure. The second step is to have a security policy requiring monthly security scans through the third-party vendor’s application software. The third step involves access control by enforcing limited access to all systems and its information for all employees.

Moreover, Participant CS-2 answered,

As a top priority, small business owners need to analyze and find areas of their businesses, which would result in a catastrophic loss, determine alternative methods to detect and then prevent cyber attacks, and implement procedures and measures to prevent cyber attacks.

Participant CS-1 explained, “Employees are not allowed to plug in any of their phone charging devices to the systems as directed by the third-party vendor.” Participants CS-1, CS-2, CS-3, and CS-4’s written security policies documented SME owners’ awareness of potential cyber security threats induced by the various virus, malware, and ransomware

programs and the implementation of multiple methods, such as computer virus scans and operating system patch updates, to prevent data breaches. Participant CS-1's and CS-2's security documents presented one of the most effective methods for preventing cyber threats, "implementing a layered security approach" (NIST, 2015a, 2015b).

Review of Participant CS-3's security policy showed secure services for, "credit card and ACH (electronic check) payments." Additionally, review of Participant CS-4's security policy showed, "All payment information is transmitted via Secure Socket Layer (SSL) technology, encrypted into our payment gateway, and accessible only by those authorized with special access rights to such systems who are required to keep the information confidential." Of note, Participants CS-1, CS-3, and CS-4 performed hardware and software security scans and backups monthly, while Participant CS-2 took a more aggressive approach and performed daily, weekly, and monthly systems scans and backups.

Cyber security awareness. SME owners are one of the foundational contributors to economic development and employment growth (Ramayah, Ling, Taghizadeh, & Rahman, 2015); however, they are hesitant to embrace and implement new technology and may suffer from resource limitations compared to larger companies (Dahnil, Marzuki, Langgat, & Fabeil, 2014). Review of Participant CS-1's security documents showed a "comprehensive card data security solution," which encompasses electronic chip technology to authenticate consumers' cards, and end-to-end encryption and tokenization technologies to protect consumers. Review of Participant CS-2's security plan showed data encryption and "the impact of tokenization on Payment Card Industry

(PCI) compliance.” Review of Participant CS-3’s security policy stated, “Seamless integration with major website providers,” utilizing a device-independent web application. Review of Participant CS-4’s security policy showed, “Secure payment solutions, 24/7 customer support, and premium protection,” which consisted of user authentication, SSL technology, and data encryption. Each SME owner indicated not only an awareness but also the need for cyber security protection by creating and implementing a written security policy.

In addition to third-party vendors providing infrastructure resources to SME owners, SME owners utilized different risk management practices thereby limiting their liability. Each SME participant expressed awareness of potential cyber security vulnerabilities and utilized risk management strategies by relying on a third-party vendor to assume or transfer those infrastructure risks. Participant CS-3 stated, “The risk management strategy we use is to always have a good environmental, situational awareness, have an acute awareness of clients’ personal information at all times, limit access, and monitor all network, system, and user activity.”

Conversely, Participants CS-1 and CS-4 relied exclusively on their third-party vendor for evaluation and identification of cyber risks. Participant CS-1 expressed, “We rely on a third-party vendor for our business and that is why we pay monthly/yearly fees for us to securely protect our data” while Participant CS-4 indicated, “We completely rely on our third-party vendor services’ strategies to identify and evaluate our security risks. Currently, the third-party vendor absorbs the burden and risks while limiting our liability.” Participant CS-2 echoed limited liability as a risk mitigation procedure by

stating, “Reliance on a third-party is great in that it limits your liability if data was compromised using their infrastructure.” SME owners must be aware and proactive to implement new security strategies to protect their business and personal client data.

Employee training. Employee training may increase the productivity of employees in business resulting in greater adherence to company policies, increased customer satisfaction, and reduction in employee turnover. Bryant and Allen (2013) reported organizations benefit from proactively managing career paths and opportunities, and leaders need to communicate with their employees about these opportunities. Participants CS-1 and CS-2 had similar approaches. Their training methodologies for employees were basic, intuitive, and updated as required. Participant CS-2 confirmed, “My employee training strategy consists of basic employee policies for operating computers and devices at the store.” Participants CS-1, CS-2, and CS-3 not only provide employee training, they also rely on vendor provided training on any new features. Once the owners receive education on new features, they conduct employee training to communicate and instruct employees on the latest software and system features. Participant CS-4 stated, “I rely primarily on vendor provided training.”

My analysis of each SME owner’s security plan and interview responses indicated vendor, employer, and on the job training were the SME owners’ preferred methods of training subthemes and are essential to SME owners’ adherence to cyber security policies, risk exposure, and liability for a data breach. First, third-party vendors provided SME owners training to understand the vendor provided business operations applications and recommended security procedures. Participant CS-1 stated, “The third-party vendor

provides a two-hour class on updating the price changes within the system.” Secondly, SME owners provided employees comprehensive on the job training covering system operations accesses, employee responsibilities, and security risks. Review of Participant CS-1’s security plan indicated third-party training and customer support. Participant CS-2 reported, “My employee training strategies consist of basic employee policies for operating computers and devices at the store.” Additionally, Participant CS-2’s security plan indicated employees must adhere to “all company policies and procedures.”

Finally, SME owners conducted periodic training as needed to ensure explicit awareness and compliance with established security policies. Participant CS-3’s interview analysis highlighted, “I provide training to our employees on gaining access to our business systems to ensure they understand the proper use of the system(s), which ultimately, lowers our potential risk exposure for security issues.” Review of Participant CS-3’s security plan highlighted payment with ease, “because of the support team.” Participant CS-4’s security plan indicated, “For network security purposes and to ensure that our services remain available to all users, we employ commercial software programs to monitor network traffic and attempt to identify unauthorized attempts to upload or change information, or otherwise cause damage.” For SME owners, an integral part of successful business operations is appropriate training for all business staff members. Figure 4 shows the data analysis results of the SME owners’ preferred methods for employee training.

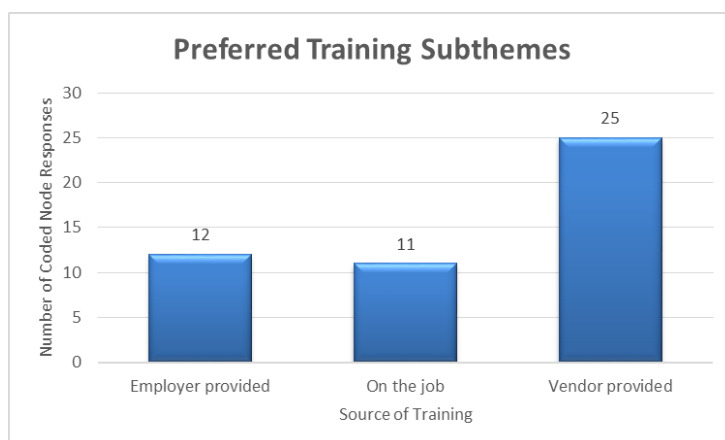


Figure 4. SME owners' preferred employee training methods.

Implementing security procedures. Loss of data affects businesses and has the potential to jeopardize a company's reputation with customers, suppliers, and partners (SBA, 2014). Media reports have cited government security offices reporting incidences of cyber crimes are on the rise and increasing daily as savvy and persistent information communication attackers find creative ways to penetrate laptops, phones, computer networks, and anything considered a wired device (FCC, 2014). Each of the participants shared a common theme in which they subscribe to system monitoring and reporting of normal and suspicious activity. Participant CS-2 stated, "My POS vendor provides different monitoring tools, which they will use to ping your IP address and try to breach security at the business through your router and firewall ports." Additionally, Participant CS-3 reiterated, "Our cyber attack contingency plan consists of ensuring our firewalls measures are up to standard. We review and monitor our systems by examining scan logs to ensure nothing strange or out of the ordinary is occurring." On the other hand, Participants CS-1 and CS-4 rely on third-party vendors for monitoring and reporting.

Theme 2: Reliance on Third-Party Vendors

The second major theme to emerge during data analysis was the reliance on third-party vendors to provide for infrastructure services and cyber security preventative measures. Data analysis uncovered the lack of sufficient in-house cyber security knowledge, skills, and abilities, and the need to utilize third-party vendors to provide expert infrastructure and cyber security protection. Each of the SME owners in this research study reported dependence and reliance on third-party vendor services to protect their businesses from cyber attacks. Review of security and privacy procedures for Participants CS-1, CS-2, and CS-3 showed SME owners adhere to the “Payment Card Industry Data Security Standards (PCI-DSS), which regulate security and safeguarding of payment cardholder data,” while Participant CS-4 adheres to SSL technologies.

Participant CS-1 stressed, “A third-party vendor limits our liability.” Likewise, Participant CS-3 indicated, “The third-party vendor minimizes our financial liability, provides protection against a data breach, and provides a warranty against losses should one occur.” Participant CS-2 confirmed similar reliance on the third-party vendor’s infrastructure resources stating, “It is difficult for a small business owner like myself to analyze and implement every aspect of a quality cyber security plan mainly due to limited resources.” Moreover, Participant CS-4 affirmed, “The benefits of outsourcing to a third-party service provider certainly outweigh the risks and liability of maintaining your infrastructure.”

Likewise, Participant CS-2 acknowledged reliance on third-party vendors by stating, “Even if you have the knowledge, skills, and resources to perform and maintain

your infrastructure, at some point, you will rely on a third-party service for some aspect of your business.” Subthemes within a SME owner’s reliance on third-party vendors included (a) hiring a secure and trusted third-party provider, (b) limiting SME owner liabilities, (c) limiting risk exposure, and (d) leveraging expert technical support for infrastructure services and cyber security protection. Figure 5 indicates SME owners’ reliance on third-party vendors.

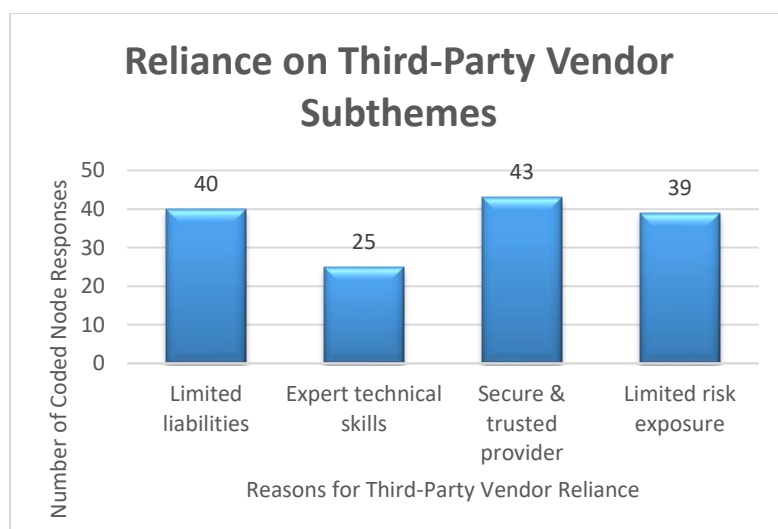


Figure 5. SME owners’ reliance on third-party vendor subthemes.

Hiring a secure and trusted third-party provider. Hiring a third-party vendor reduces SME owners’ liabilities, and Participant CS-1 disclosed, “We do not have the knowledge, resources, and people to perform these functions ourselves and that is why we leverage a third-party vendor.” Participant CS-2 stressed, “SME owners should also consider hiring a network company or third-party vendor to handle protecting their business infrastructure.” Moreover, Participant CS-1 indicated, “We use third-party vendors and rely on their services for our business” while Participant CS-3 echoed

agreement, “The first step is prevention by utilizing a third-party vendor’s infrastructure.” Moreover, Participant CS-4 stated, “Our third-party vendor provides the basis we use for our small business infrastructure, and we trust them.”

Limited liabilities. Business owners’ defense methodologies should focus on mitigating risks associated with owning and operating information systems (FCC, 2014; Jang-Jaccard & Nepal, 2014). Different views for implementing loose and strong password criteria depend on the business model and user/customer base willingness and ease to access desired technology. J. Hong and Reed (2013) reviewed password guidelines for retailers such as Amazon, Fidelity Investments, and PayPal, which revealed loose password policies and products without stringent verifications.

In response to SME owners’ responsibilities and liabilities, if a data breach were to occur, each of the participants utilizes a third-party service, which limits their liability if a data breach occurs. Participant CS-1 replied, “With a third-party vendor we have limited liability.” It is imperative for business owners to develop and implement cyber security strategies and preventative measures to mitigate data losses (FBI, 2015a). SME owners who utilize third-party vendors limit their cyber security liabilities and thwart catastrophic cyber security losses. Participant CS-4 conveyed, “The third-party vendor service provider maintains the confidentiality of the clients’ information and payment credentials, and are liable for data loss should one occur.” Likewise, Participants CS-2 and CS-3 interview responses revealed they do not write down or store within their businesses their customers’ credit card numbers.

Participant CS-4 indicated, “Our contingency plan for our small business is to rely on our third-party vendor to provide the infrastructure, and if a data breach were to occur, they would inform us of the cyber security breach.” Likewise, Participant CS-1 affirmed, “Our cyber attack contingency plan is to immediately call our third-party vendor. We rely on our third-party vendor for our business, and that is why we pay monthly/yearly fees for us to securely protect our data.”

Limited risk exposure. Managing cyber risks requires organizations to implement multitiered security strategies focused on prevention, mitigation, and reaction while concentrating on people, processes, and systems (NIST, 2015a, 2015b). The study participants expressed an awareness of potential cyber security vulnerabilities and utilized risk management strategies by relying on third-party vendors for infrastructure risks. Participant CS-1’s interview response reflected, “With a third-party vendor we have limited liability.” Review of Participant CS-1’s security plan showed the third-party vendor provided an, “unprecedented breach warranty” at no additional cost.

Participant CS-2’s interview response stated, “Reliance on a third-party is great in that it limits your liability if data was compromised using their infrastructure.” Review of Participant CS-2’s security plan showed payment transactions were, “backed by a comprehensive warranty.” Participant CS-3’s interview response recommended other SME owners keep “Computer and operating systems up to date with the latest security patches, leveraging the encrypted cloud computing technologies and services, and instilling employee security awareness by implementing security policies and procedures.” Additionally, Participant CS-3’s implementation of a written security

policy showed adherence to protecting customer data through “security and safeguarding of payment cardholder data.”

Business owners should concentrate their efforts to reduce risks by implementing technical and political solutions (NIST, 2015b; SBA, 2015, 2016b). Moreover, Participant CS-4 declared, “The benefits of outsourcing to a third-party service provider certainly outweigh the risks and liability of maintaining your infrastructure.” Review of Participant CS-4’s security documents showed limited warranty services, which are remedied and “limited to a claim.” The study participants’ interview responses confirmed SME owners outsource infrastructure and resources to support their secure business operations.

Expert technical skills. According to the SBA (2014) and the SEC (2015), SME owners are predominantly disadvantaged in protecting their infrastructures against cyber attacks. The adoption of cloud computing has many benefits enabling SME owners to compete globally in a cost effective manner with seamless sharing of cloud infrastructure and computing resources. Strategic planning elements should include how organizations can leverage emerging technologies to assist with their strategic visions and risk assessments (NIST, 2015b). Cyber security threats are continuously evolving requiring vigilant awareness.

Participant CS-1 stated, “We use third-party vendors and rely on their services for our business.” Additionally, review of Participant CS-1’s archival documents indicated their company has the, “Most secure credit card processing solution on the market, backed by a comprehensive breach warranty.” Both Participants CS-2 and CS-3 stressed

the importance of keeping their computer operating systems up to date with their vendor's latest security patches, knowing the operating system well and being able to install and reinstall operating and software systems if necessary, and limiting access to systems and sensitive information via unique logins and passwords. Participant CS-4's interview response reported, "We utilize our third-party vendor to provide the infrastructure for protecting, detecting, and responding to cyber threats." Moreover, review of Participant CS-4's archival documents indicated their company received praise for innovation in providing secure business solutions and featured on major news outlets.

Theme 3: Cyber Security Awareness

Consumer advocacy groups promote increasing user and business awareness and taking steps to reduce risk exposure (DHS, 2015a; FCC, 2014; SBA, 2014). The third major theme to emerge during data analysis was ensuring cyber security awareness. Creating awareness about security issues is imperative for an organization's overall objective to implement an effective security program (Mishra, Caputo, Leone, Kohun, & Draus, 2014). Additionally, Mishra et al. (2014) identified training and education as effective methods to create awareness of security vulnerabilities since these make employees aware of the risks and their responsibilities to protect infrastructure assets. Organizational leaders must implement a tailored set of focus areas and capabilities to reach a high-security maturity level (Mijnhardt, Baars, & Spruit, 2016). The data analysis showed each of the participants in this research study corroborated Mishra et al. affirming cyber security awareness is a critical component of their effective cyber security strategy.

Miles (2013) reported the focus of systems theory relies heavily on the interconnectivity between the parts as well as the relationship between the parts that connect them together. Successful SME owners are aware of their diverse globally changing environment necessitating the requirement for cyber security awareness. Data analysis of archival documents and interview responses revealed three primary cyber security awareness subthemes (a) knowledge of protection, (b) knowledge of third-party vendors, and (c) knowledge of strategic plans. Figure 6 shows the SME owners' cyber security awareness subthemes.

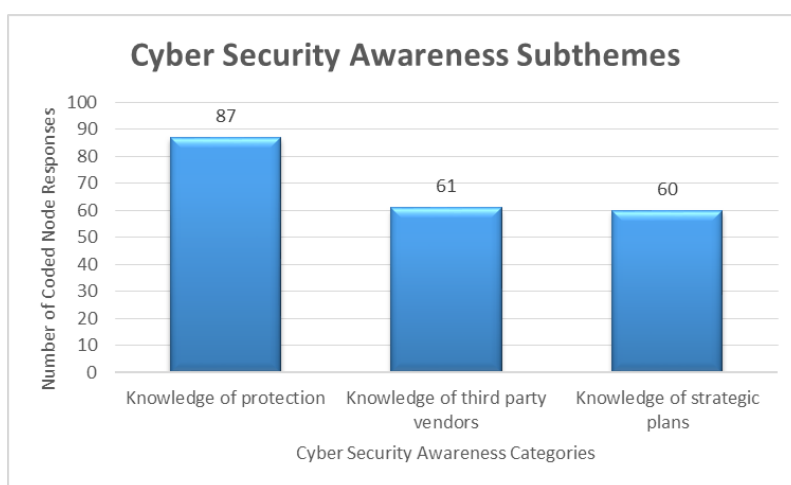


Figure 6. SME owners' cyber security awareness subthemes.

Knowledge of protection. Hayes and Bodhani (2013) stressed SME owners must be more aware of cyber security if they are going to avoid becoming cyber victim casualties. Ultimately, a business owner must evaluate whether the risks of outsourcing security protection services to a third-party are necessary to mitigate company losses (FBI, 2014, 2015c). The data analysis of archival documents and interview responses illustrated knowledge of protection as the most predominant coded node response.

Review of archival documents for Participants CS-1 and CS-2 indicated the use of secure tokenization services to protect client data by “replacing sensitive data like credit card numbers with tokens.”

Participant CS-1 stated, “We have the point of sale system (POS) that processes payments using data encryption,” and recommended, “Other small business owners to do their research on POS and third-party infrastructure providers.” Likewise, Participant CS-2 stated, “As a minimum, small businesses must identify and protect data that if lost would result in a catastrophic failure of the business.” Furthermore, Participant CS-2 discussed the need to conduct “Random scenarios to test the business contingency plan. I recently had the POS vendor review the backup database files for data integrity and whether the files could be used successfully for a full restore.”

Participant CS-3 acknowledged, “We depend on our third-party vendor’s infrastructure to access our systems. Access to our systems is through firewalls and encrypted routers.” Additionally, Participant CS-3 stated, “We have a security policy requiring monthly security scans through the third-party vendor’s application software.” Analysis of Participant CS-3’s archival documents indicated the third-party vendor have, “more than 60 years of combined experience in payment processing, billing, and electronic finances.” Participant CS-4 reiterated, “The successful strategies we use to protect our small business infrastructure from cyber attacks rely on contracting out and working through a third-party service provider.” Review of Participant CS-4’s archival documents reflected, “We employ commercial software programs to monitor network traffic and attempt to identify unauthorized attempts to upload or change information, or

otherwise cause damage.” One of the biggest issues facing SME owners is the ability to defend themselves from potential cyber attacks (Fielder et al., 2016).

Knowledge of third-party vendors. SME owners are more vulnerable to cyber attacks than large enterprises because they may lack the IT expertise and resources needed to understand and confront IT security issues in the rapidly growing threat environments (Emm, 2013). The findings of the study reveal each SME participant is reliant on a third-party vendor to provide infrastructure support to their business. Secure and trusted third-party providers, vendor training, limited liability, and risk reduction measures are essential elements SME owners leverage when relying on third-party vendor services.

While dependence and reliance on third-party vendors is a subtheme of cyber security awareness, it is also one of the three major emergent themes resulting from data analysis. Participant CS-1 reported, “We do not have the knowledge, resources, and people to perform these functions ourselves and that is why we leverage a third-party vendor. We trust these providers to protect our data as that is what they do.” Review of Participant CS-1’s and CS-2’s archival documents indicates the services are secure, reliable, scalable, and utilize “proprietary POS security technology to provide unparalleled protection.” Participant CS-2 indicated, “I rely on PCI compliance strategies, despite being a bit annoying; this standard provides a level of comfort and limits my liability.” Review of Participant CS-3’s archival documents indicates the third-party vendor provides secure services, “unmatched customer service,” and are “exceptionally knowledgeable in credit card and ACH (electronic check) payments.”

Likewise, Participant CS-3 affirmed, “Using a third-party vendor minimizes our financial liability, provides protection against a data breach, and provides a warranty against losses should one occur.”

Participant CS-4 stated, “We utilize our third-party vendor to provide the infrastructure for protecting, detecting, and responding to cyber threats.” Additionally, Participant CS-4 stated, “We use this third-party vendor because they host our entire website and customer payments are accepted and processed via their secure encryption methods.” Review of Participant CS-4’s archival documents reiterated, “All payment information is transmitted via Secure Socket Layer (SSL) technology, encrypted into our payment gateway, and accessible only by those authorized with special access.”

Knowledge of strategic plans. SME owners must take a proactive approach to protect their data by establishing cyber security plans, and create and implement Internet security policies (DHS, 2015b; SBA, 2014). The data analysis of archival documents and interview responses showed the SME owners’ requirement for strategic plans the third most important factor within the cyber awareness subthemes. SME owners cannot achieve competitiveness and remain profitable without adopting new technologies at the right market stages (Maduku, Mpinganjira, & Duh, 2016). SME owners may utilize multiple marketing techniques such as Internet websites, social media, Facebook, or Twitter, to advertise and obtain customers.

Dahnil et al. (2014) characterized social media as a new marketing communication tool whereby businesses are leveraging multiple social media venues to enhance their marketing efforts and gain entrance into global competitive markets.

Developing a system of preventive security measures adds a significant deterrent to protect networks from malicious cyber activity (DHS, 2015b; SBA, 2014). Sheppard et al. (2013) emphasized both public and private organizations require a robust cyber security strategic approach to prepare, respond, and recover from cyber attacks.

Another critical element of strategic plans entails an evaluation of vulnerabilities. A common element echoed by analyzing participants' interview responses reflected the need to establish and implement a viable strategic plan encompassing multiple types of cyber security protection. Participant CS-1 stated, "All of our servers are password protected, and we enable employees to either use their password or utilize employee fingerprint recognition to log into our systems." Review of Participant CS-1's, CS-2's, CS-3's, and CS-4's archival documents indicated the existence of strategic plans that include cyber security protection. Participant CS-2 replied, "My third-party POS vendor uses a PCI questionnaire, which gets me thinking about different things which could cause cyber threats and provokes different thoughts on how to prevent a data breach or attack."

Developing and implementing a security plan is another key strategic initiative. Participant CS-3 stated, "The successful strategies that we use to protect our business infrastructure from a cyber attack consist of leveraging a third-party vendor's cyber security solution." Participant CS-4 stressed, "Our third-party vendor service provider maintains the confidentiality of the client's information and payment credentials, and they are liable for data loss should one occur." NIST (2015b) emphasized cyber security decisions require insight into current security threats and the ability to forecast potential

vulnerabilities. SME owners who implement security awareness practices may increase employees' awareness against potential cyber security threats.

Applications to Professional Practice

The findings of this study, along with the results of the analysis of the study's conceptual framework and extensive review of scholarly literature, add to the existing body of knowledge to improve SME owners' secure business operations. Based on the study findings, the most significant contribution may be the identification of SME owners' implementation of cyber security best practices to protect their businesses from cyber attacks. Choucri, Madnick, and Ferwerda (2014) reported implementing best practices would help mitigate cyber threats.

My findings from the research study indicated successful SME owners effectively apply three major strategies to protect their businesses from cyber attacks. The most frequently used technique SME owners use consists of developing and implementing a comprehensive strategic plan to alleviate cyber security threats and data breaches. The successful strategic plans included (a) limiting system access through password protection methods, (b) establishing a cyber security plan, (c) ensuring cyber security awareness, (d) conducting training, and (e) implementing security procedures. The strategic plan is critical because it provides the foundation for secure business operations.

The second most frequently used strategy successful SME owners apply includes the reliance on third-party vendors to provide expert infrastructure and cyber security protection. Data analysis revealed the lack of sufficient in-house cyber security knowledge, skills, and abilities, and the need to utilize a secure and trusted third-party

supplier. Each of the SME owners in this research study reported dependence and reliance on third-party vendor services to protect their businesses from cyber attacks. The successful strategic plans included (a) hiring a secure and trusted third-party provider, (b) limiting the SME owner's liabilities, (c) limiting risk exposure, and (d) leveraging expert technical support for infrastructure services and cyber security protection.

The third most frequently used strategy successful SME owners apply is cyber security awareness. Mishra et al. (2014) emphasized creating awareness about security issues is imperative for an organization's overall objective to implement an effective security program. The successful strategic plans incorporated (a) knowledge of protection, (b) knowledge of third-party vendors, and (c) knowledge of strategic plans. The data analysis showed each of the participants in this research study corroborated Mishra et al. affirming cyber security awareness is a critical component of their effective cyber security strategy.

The application to professional practice includes the communication of successful SME owners' strategies to protect their businesses against cyber threats and thwart potential cyber attacks. The results of my research indicate the application of effective SME owners' cyber security strategies might provide other SME owners a foundational guide to assess and mitigate cyber threat vulnerabilities. The findings in my study align with the systems theory whereby successful SME owners leverage the three major strategies together for more effective, secure, and sustainable business operations.

Implications for Social Change

The implications for social change from this research include the potential impact of successful cyber security strategies for SME owners to mitigate and prevent future cyber security attacks. One of the biggest issues facing SME owners is the ability to defend themselves from potential cyber attacks (Fielder et al., 2016). Implementation of effective cyber security best practices, as outlined in the research study findings, provides SME owners increased knowledge of cyber security methodologies, provides sustainable cyber security strategies to mitigate future cyber attacks, and enhances their potential for sustainable business operations. This qualitative multicase study filled a gap in the related literature by providing additional perspectives on successful SME owners' cyber security strategies within a globally changing environment.

Findings from the study have provided SME owners with three effective strategies successful SME owners use to prevent cyber security attacks (a) cyber security strategy, (b) reliance on third-party vendors for infrastructure services, and (c) cyber security awareness. Application of these strategies may catalyze consumer confidence resulting in greater economic prosperity. The implications for positive social change include empowering other SME owners, new entrepreneurs, and academic institutions with successful strategies and resources to effect changes within the community. Additionally, SME owners may transform the way they view cyber security strategies, expand businesses, and assist other SME owners who survive cyber attacks spur economic growth by employing residents of the community stimulating the overall socioeconomic lifecycle.

Recommendations for Action

The purpose of this qualitative multicase study was to explore effective strategies successful SME owners use to protect their businesses from cyber attacks. SME owners represent 99.7% of U.S. employers (U.S. Census Bureau, 2013). In 2014, 60% of all targeted cyber attacks struck SMEs whose owners are predominantly disadvantaged in protecting their infrastructures (Symantec Corporation, 2015; United States Securities and Exchange Commission [SEC], 2015). SME owners do not view themselves as targets of cyber attacks due to their small size or the perception they have nothing worth stealing (SBA, 2015).

This research study concentrated on the analysis of scholarly literature, archival documents, and SME owners' participant interview member checked responses, which provided corroborative support and triangulation in the data collection process, to answer the research question of what effective strategies SME owners use to protect their businesses from cyber attacks. Three major themes emerged from the triangulated data analysis, based on the frequencies of coded node responses: (a) cyber security strategy, (b) reliance on third-party vendors for infrastructure services, and (c) cyber security awareness. The findings of this research study indicate SME owners (a) have implemented cyber security policies to protect, defend, and react to cyber attacks; (b) rely on third-party vendors to provide infrastructure services and cyber security protection; and (c) are aware of cyber security threats.

Based on unique, successful strategies SME owners use to prevent cyber attacks, I recommend business owners, future business owners, and new entrepreneurs consider the following actions to secure information through best cyber security practices:

1. Assess cyber security health by evaluating the current cyber threat environment; identify the types of business data to protect; pinpoint insider and outsider threats, risks and vulnerabilities; and highlight types of possible cyber threats.
2. Develop and implement a comprehensive cyber security strategic plan, which includes policies and procedures to protect sensitive and potentially sensitive data.

The cyber security strategic plan should at a minimum establish:

- a. Valid user two-factor authentication (login and password);
 - b. Company computers equipped with antivirus software, antispymware, and malware software; and computer operating system patches kept current;
 - c. Secure Internet and Wi-Fi network connections using firewalls and data encryption methodologies;
 - d. End-to-end data encryption and tokenization for secure business transactions; and
 - e. Protected company business websites using secure features for data transactions (such as firewalls, routers, SSL, and PCI data compliance).
3. Assess in-house IT capabilities and consider employing third-party vendors to leverage their expert skills, reduce infrastructure risks and liabilities, and mitigate potential data breach losses by utilizing the third-party vendor's cyber security data breach warranty.

4. Ensure cyber security awareness by training employees on company policies for data protection, protection of business and consumer data, and daily rules of engagement for secure, successful business operations.

I plan to disseminate the results and recommendations from this study by providing summary fact sheets to the four SME owners who participated in the study. I will offer my consultant services as a guest speaker for the Melbourne Regional Chamber of Commerce for East Central Florida, the Space Coast Tech Council (SCTC), and the IT and Entrepreneur subcommittee to discuss my research findings and its applicability to businesses and interested parties in the local area. Additionally, I will make an effort to share the results and recommendations of the study with academic institutions in the local area such as Eastern Florida State College (EFSC) and Florida Institute of Technology (FIT), as a guest speaker for seminars and workshops. I will also provide my consultant services as a guest speaker on successful SME owners' cyber security strategies for government, such as the Brevard County EDC, and nongovernment-sponsored conferences and workshops for SME owners needing assistance. Moreover, I will seek to disseminate my research findings through industry publications and academic journals.

Recommendations for Further Research

The findings, conclusions, and recommendations from this study may contribute to existing, and future research regarding best practices owners of SME businesses use to protect and defend their businesses from cyber attacks to achieve successful, sustainable business operations. Since this study was limited to the metropolitan area of Melbourne, Brevard County, Florida, I would recommend a study based in a different geographic

location, to see if the findings will be similar or different based on regional data. Additionally, since the sample population for this study was four owners of SME businesses, I would recommend future researchers expand the sample size to determine if results would be similar or different based on sample size.

Section 1 limitations addressed whether participants would understand the interview questions and provide honest answers, participants' availability for personal interviews to support timely data collection, and whether reviewing archival company documents and conducting semistructured interviews would provide sufficient data to answer the overarching research question. The only limiting factor that affected the research endeavors was finding owners of SME businesses in the Melbourne, Brevard County, Florida, metropolitan area who were willing to participate in the research study, which significantly increased the amount of time I spent obtaining viable research participants. However, once SME owners agreed to participate, there were no significant issues. Archival data was available, and interviews yielded candid participant responses to provide sufficient data for analyses. I would recommend future researchers consider allotting additional time to obtain viable research participants.

Reflections

Completing the DBA Doctoral Study process has been a rewarding growth experience. The journey challenged me academically and personally far beyond what I had anticipated. I have significantly increased my knowledge of effective cyber security strategies successful SME owners use to protect their businesses from cyber security threats; specifically SME owners in the Brevard County, Florida, metropolitan area. I am

confident I can share the application of my research findings with scholars, academic institutions, business owners, entrepreneurs, and government entities. The findings of the research study may contribute to existing, and future research regarding best practices SME owners use to protect and defend their businesses from cyber attacks to achieve more successful sustainable, secure business operations.

A personal bias after conducting the literary research was a preconceived notion the majority of SME owners were not aware of and did not practice adequate cyber security solutions to address potential cyber threat vulnerabilities. Additionally, my experience as an IT subject matter expert and program manager for a large corporation, which utilizes extensive, effective cyber security practices fueled this idea. Each of the participants was a successful SME owner, cognizant of cyber threat vulnerabilities and potential consequences to their secure business operations. During the semistructured interviews, I took special care not to lead the participants nor show positive or negative reactions to their responses. I am confident the respondents provided honest, candid answers to the eight questions and my actions did not adversely influence their responses.

After completing the research study, my preconceived notion changed regarding successful SME owners' serendipitous use of effective cyber security strategies. The literature review provided results that indicated high costs and risks for using third-party vendors. After completing the data analysis of archival documents and participant interviews, my thinking changed. Successful SME owners evaluated their risks and determined third-party vendors were adaptable, scalable, cost-effective, provided expert technical and infrastructure services, and limited their liabilities in case of data breaches.

Although this research study focused on a small population in central Florida, perhaps the results of the study are indicative successful SME owners in other geographical areas have implemented similar strategic actions to prevent cyber security threats.

Conclusion

The purpose of this qualitative multiple case study was to explore what strategies successful SME owners use to protect their businesses from cyber attacks. The findings of this research study elucidate effective strategies SME owners use to protect their businesses from cyber attacks. Three main themes emerged from the research findings, which correlated with the literature review, the existing body of knowledge, and the conceptual framework of the GST. The findings of this research study are SME owners (a) have implemented cyber security policies to protect, defend, and react to cyber attacks; (b) rely on third-party vendors to provide infrastructure services and cyber security protection; and (c) are aware of cyber security threats. SME owners who survive cyber attacks may spur economic growth by employing residents of the community stimulating the socioeconomic lifecycle. Moreover, SME owners' implementation of these successful strategies may catalyze consumer confidence resulting in greater economic prosperity. The reality of the ever changing global cyber security threat environment mandates SME owners assess vulnerabilities, and develop and implement cyber security best practice strategies to ensure secure sustainable business operations.

References

- Aaltonen, A., & Tempini, N. (2014). Everything counts in large amounts: A critical realist case study on data-based production. *Journal of Information Technology*, 29, 97-110. doi:10.1057/jit.2013.29
- Abbe, A., & Brandon, S. E. (2013). The role of rapport in investigative interviewing: A review. *Journal of Investigative Psychology & Offender Profiling*, 10, 237-249. doi:10.1002/jip.1386
- Abdellaoui, A., Khamlichi, Y. I., & Chaoui, H. (2016). A BYOD method for enhancing authentication in the cloud environment using elliptic curves. *International Journal of Computer Science and Information Security*, 14(5), 63. Retrieved from <https://sites.google.com/site/ijcsis/>
- Abma, T. A., & Stake, R. E. (2014). Science of the particular an advocacy of naturalistic case study in health research. *Qualitative Health Research*, 24, 1150-1161. doi:10.1177/1049732314543196
- Allen, B. J., & Garg, K. (2016). Diversity matters in academic radiology: Acknowledging and addressing unconscious bias. *Journal of the American College of Radiology*, 13, 1426-1432. doi:10.1016/j.jacr.2016.08.016
- Alshenqeeti, H. (2014). Interviewing as a data collection method: A critical review. *English Linguistics Research*, 3(1), 39-45. doi:10.5430/elr.v3n1p39
- Arief, B., Bin Adzmi, M. A., & Gross, T. (2015). Understanding cybercrime from its stakeholders' perspectives: Part 1 - attackers. *IEEE Security & Privacy*, 13(1), 71-76. doi:10.1109/MSP.2015.19

- Arlitsch, K., & Edelman, A. (2014). Staying safe: Cyber security for people and organizations. *Journal of Library Administration*, 54(1), 46-56.
doi:10.1080/01930826.2014.893116
- Askitas, N., & Zimmermann, K. F. (2015). The Internet as a data source for advancement in social sciences. *International Journal of Manpower*, 36, 2-12.
doi:10.1108/IJM-02-2015-0029
- Atoum, I., & Otoom, A. (2016). Holistic performance model for cyber security implementation frameworks. *International Journal of Security and Its Applications*, 10(3), 111-120. doi:10.14257/ij sia.2016.10.3.10
- Avgerinos, T., Cha, S. K., Rebert, A., Schwartz, E. J., Woo, M., & Brumley, D. (2014). Automatic exploit generation. *Communications of the ACM*, 57(2), 74-84.
doi:10.1145/2560217.2560219
- Azhar, S., Latif, U., Murtaza, G., Khan, S. A., & Hussain, I. (2013). Mixed methodology approach in pharmacy practice research. *Acta Poloniae Pharmaceutica*, 70, 1123-1130. Retrieved from <http://www.ptfarm.pl>
- Bambauer, D. E. (2013). Ghost in the network. *University of Pennsylvania Law Review*, 162, 1011-1091. Retrieved from <http://scholarship.law.upenn.edu/>
- Barratt, M. J., Ferris, J. A., & Lenton, S. (2015). Hidden populations, online purposive sampling, and external validity taking off the blindfold. *Field Methods*, 27, 3-21.
doi:10.1177/1525822X14526838
- Baškarada, S. (2014). Qualitative case study guidelines. *The Qualitative Report*, 19(40), 1-25. Retrieved from <http://nsuworks.nova.edu/tqr/>

- Betz, D. J., & Stevens, T. (2013). Analogical reasoning and cyber security. *Security Dialogue*, 44, 147-164. doi:10.1177/0967010613478323
- Black, S. A., & Copsey, J. A. (2014). Does Deming's "system of profound knowledge" apply to leaders of biodiversity conservation? *Open Journal of Leadership*, 3, 53-65. doi:10.4236/ojl.2014.32006
- Boblin, S. L., Ireland, S., Kirkpatrick, H., & Robertson, K. (2013). Using Stake's qualitative case study approach to explore implementation evidence-based practice. *Qualitative Health Research*, 23, 1267-1275. doi:10.1177/1049732313502128
- Boddy, C. R. (2016). Sample size for qualitative research. *Qualitative Market Research: An International Journal*, 19, 426-432. doi:10.1108/QMR-06-2016-0053
- Bodhani, A. (2013). Turn on, log in, checkout. *Engineering & Technology*, 8, 60-63. doi:10.1049/et.2013.0308
- Bowden, C., & Galindo-Gonzalez, S. (2015). Interviewing when you're not face-to-face: The use of email interviews in a phenomenological study. *International Journal of Doctoral Studies*, 10, 79-92. Retrieved from <http://ijds.org/>
- Brevard County Tax Collector. (2014, November 30). *Brevard tax collector*. Titusville, FL. Retrieved from <http://www.brevardtaxcollector.com/>
- Bridges-Rhoades, S., & Van Cleave, J. (2014). Pursuing responsibility writing and citing subjects in qualitative research, *Qualitative Inquiry*, 20, 641-652. doi:10.1177/1077800413513724

- Brody, B., Migueles, S. A., & Wendler, D. (2015). Should all research subjects be treated the same? *Hastings Center Report*, 45(1), 17-20. doi:10.1002/hast.414
- Brooks, J. S., & Normore, A. H. (2015). Qualitative research and educational leadership: Essential dynamics to consider when designing and conducting studies. *International Journal of Educational Management*, 29, 798-806. doi:10.1108/IJEM-06-2015-0083
- Bryant, P. C., & Allen, D. G. (2013). Compensation, benefits, employee turnover: HR strategies for retaining top talent. *Compensation & Benefits Review*, 45(3), 171-175. doi:10.1177/0886368713494342
- Burley, D. L., Eisenberg, J., & Goodman, S. E. (2014). Would cybersecurity professionalization help address the cybersecurity crisis? *Communications of the ACM*, 57(2), 24-27. doi:10.1145/2556936
- Campbell-Kelly, M., & Garcia-Swartz, D. D. (2013). The history of the Internet: The missing narratives. *Journal of Information Technology*, 28, 18-33. doi:10.1057/jit.2013.4
- Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J., & Neville, A. J. (2014). The use of triangulation in qualitative research. *Oncology Nursing Forum*, 41, 545-547. doi:10.1188/14.onf.545-547
- Castleberry, A. (2014). NVivo 10 [software program]. Version 10. QSR international; 2012. *American Journal of Pharmaceutical Education*, 78, 25. doi:10.5688/ajpe78125

- Caws, P. (2015). General systems theory: Its past and potential. *Systems Research and Behavioral Science*, 32, 514-521. doi:10.1002/sres.2353
- Central Intelligence Agency [CIA]. (2015). *The world fact book: Internet users*. Washington, DC. Retrieved from <https://www.cia.gov/index.html>
- Chang, J., Venkatasubramanian, K. K., West, A. G., & Lee, I. (2013). Analyzing and defending against web-based malware. *ACM Computing Surveys*, 45(4), 1-35. doi:10.1145/2501654.2501663
- Chen, Y., Wang, Y., Nevo, S., Jin, J., Wang, L., & Chow, W. S. (2014). IT capability and organizational performance: The roles of business process agility and environmental factors. *European Journal of Information Systems*, 23, 326-342. doi:10.1057/ejis.2013.4
- Cheswick, W. (2013). Rethinking passwords. *Communications of the ACM*, 56(2), 40-44. doi:10.1145/2408776.2408790
- Chiumento, A., Khan, M. N., Rahman, A., & Frith, L. (2015). Managing ethical challenges to mental health research in post conflict settings. *Developing World Bioethics*, 16, 15-28. doi:10.1111/dewb.12076
- Choucri, N., Madnick, S., & Ferwerda, J. (2014). Institutions for cyber security: International responses and global imperatives. *Information Technology for Development*, 20, 96-121. doi:10.1080/02681102.2013.836699
- Chou, T.-S. (2013). Security threats on cloud computing vulnerabilities. *International Journal of Computer Science and Information Technology*, 5, 79-88. doi:10.5121/ijcsit.2013.5306

- Chowdappa, K. B., Lakshmi, S. S., & Kumar, P. P. (2014). Ethical hacking techniques with penetration testing. *International Journal of Computer Science and Information Technologies*, 5, 3389-3393. Retrieved from <http://www.ijcsit.com/>
- Chua, Y. T., & Holt, T. J. (2016). A cross-national examination of the techniques of neutralization to account for hacking behaviors. *Victims & Offenders*, 11(4), 534–555. doi:10.1080/15564886.2015.1121944
- City of Melbourne, The Harbor City. (2016, January 15). *About the city of Melbourne*. Retrieved from <http://www.melbourneflorida.org/about>
- Cleary, M., Horsfall, J., & Hayter, M. (2014). Data collection and sampling in qualitative research: Does size matter? *Journal of Advanced Nursing*, 70, 473-475. doi:10.1111/jan.12163
- Communications of the ACM (CACM) Staff. (2013). Plenty more hacker motivations. *Communications of the ACM*, 56(7), 8-9. doi:10.1145/2483852.2483856
- Cronin, C. (2014). Using case study research as a rigorous form of inquiry. *Nurse Researcher*, 21(5), 19-27. Retrieved from <http://rcnpublishing.com/journal/nr>
- Dahnil, M. I., Marzuki, K. M., Langgat, J., & Fabeil, N. F. (2014). Factors influencing SMEs adoption of social media marketing. *Procedia - Social and Behavioral Sciences*, 148, 119-126. doi:10.1016/j.sbspro.2014.07.025
- Deakin, H., & Wakefield, K. (2013). Skype interviewing: Reflections of two PhD researchers. *Qualitative Research*, 14, 603-616. doi:10.1177/1468794113488126
- Denning, T., Kohno, T., & Levy, H. M. (2013). Computer security and the modern home. *Communications of the ACM*, 56(1), 94-103. doi:10.1145/2398356.2398377

- Denzin, N. K. (2012). Triangulation 2.0. *Journal of Mixed Methods Research*, 6, 80-88.
doi:10.1177/1558689812437186
- Department of Defense [DoD]. (2015). *The DoD cyber strategy*. Washington, DC.
Retrieved from https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf
- Desai, D. (2013). Beyond location: Data security in the 21st century. *Communications of the ACM*, 56(1), 34-36. doi:10.1145/2398356.2398368
- Dillon, S., & Vossen, G. (2015). SaaS cloud computing in small and medium enterprises: a comparison between Germany and New Zealand. *International Journal of Information Technology, Communications and Convergence*, 3, 87-104.
doi:10.1504/ijitcc.2015.070998
- Disterer, G., & Kleiner, C. (2013). Using mobile devices with BYOD. *International Journal of Web Portals (IJWP)*, 5(4), 33-45. doi:10.4018/ijwp.2013100103
- Dunn Cavelty, M. (2013). From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. *International Studies Review*, 15, 105-122. doi:10.1111/misr.12023
- Dunn Cavelty, M. (2014). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. *Science and Engineering Ethics*, 20, 701-715.
doi:10.1007/s11948-014-9551-y
- Economic Development Commission [EDC], Florida's Space Coast. (2016). *Economic Development Commission, Florida's Space Coast*. Retrieved from <http://spacecoastedc.org/>

- Egele, M., Scholte, T., Kirda, E., & Kruegel, C. (2012). A survey on automated dynamic malware-analysis techniques and tools. *ACM Computing Surveys*, *44*(2), 1-42.
doi:10.1145/2089125.2089126
- Egidi, M. (2015). Schumpeter's picture of economic and political institutions in the light of a cognitive approach to human behavior. *Journal of Evolutionary Economics*, *25*, 1-21. doi:10.1007/s00191-015-0421-9
- Elo, S., Kääriäinen, M., Kanste, O., Pölkki, T., Utriainen, K., & Kyngäs, H. (2014). Qualitative content analysis: A focus on trustworthiness. *SAGE Open*, *4*(1), 1-10.
doi:10.1177/2158244014522633
- Embassy of the United States. (2013). *No nation can combat cybercrime alone, attorney general says*. London, UK. Retrieved from <http://london.usembassy.gov/cybersecurity008.html>
- Emm, D. (2013). Security for SMBs: Why it's not just big businesses that should be concerned. *Computer Fraud & Security*, *4*, 5-8.
doi:10.1016/S1361-3723(13)70036-8
- Ezekiel, A. W. (2013). Hackers, spies, and stolen secrets: Protecting law firms from data theft. *Harvard Journal Law and Technology*, *26*, 649-695. Retrieved from <http://jolt.law.harvard.edu/>
- Federal Bureau of Investigation [FBI]. (2013a). *Cyber crime*. Washington, DC. Retrieved from <https://www.fbi.gov/about-us/investigate/cyber>

Federal Bureau of Investigation [FBI]. (2013b). *Today's FBI facts & figures 2013-2014*.

Washington, DC. Retrieved from <https://www.fbi.gov/stats-services/publications/todays-fbi-facts-figures/facts-and-figures-031413.pdf>

Federal Bureau of Investigation [FBI]. (2014). *Responding to the cyber-threat*.

Washington, DC. Retrieved from <https://www.fbi.gov/news/testimony/responding-to-the-cyber-threat>

Federal Bureau of Investigation [FBI]. (2015a). *Internet Crime Complaint Center (IC3),*

2014 IC3 annual report. Washington, DC. Retrieved from <https://www.ic3.gov/media/annualreports.aspx>

Federal Bureau of Investigation [FBI]. (2015b). *Organized crime overview*. Washington,

DC. Retrieved from <https://www.fbi.gov/about-us/investigate/organizedcrime/overview>

Federal Bureau of Investigation [FBI]. (2015c). *Stories*. Washington, DC. Retrieved from

<https://www.fbi.gov/news/stories/2015/october/national-cyber-security-awareness-month>

Federal Bureau of Investigation [FBI]. (2016). *Stories*. Washington, DC. Retrieved from

<https://www.fbi.gov/investigate/cyber>

Federal Communications Commission [FCC]. (2014). *Cyber security planning guide*.

Washington, DC. Retrieved from <https://transition.fcc.gov/cyber/cyberplanner.pdf>

Federal Trade Commission [FTC]. (2016). *Data security*. Washington, DC. Retrieved

from <https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security>

- Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision Support Systems*, 86, 13-23. doi:10.1016/j.dss.2016.02.012
- Filshinskiy, S. (2013). Cybercrime, cyberweapons, cyber wars: Is there too much of it in the air? *Communications of the ACM*, 56(6), 28-30.
doi:10.1145/2461256.2461266
- Fletcher, D., Massis, A. D., & Nordqvist, M. (2016). Qualitative research practices and family business scholarship: A review and future research agenda. *Journal of Family Business Strategy*, 7, 8-25. doi:10.1016/j.jfbs.2015.08.001
- Fulton, E., Lawrence, C., & Clouse, S. (2013). White hats chasing black hats: Careers in IT and the skills required to get there. *Journal of Information Systems Education*, 24, 75-80. Retrieved from <http://jise.org/>
- Fusch, P. I., & Fusch, G. E. (2015). Leadership and conflict resolution on the production line. *International Journal of Applied Management and Technology*, 14(1), 21-39. Retrieved from <http://scholarworks.waldenu.edu/ijamt/>
- Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report*, 20(9), 1408-1416. Retrieved from <http://nsuworks.nova.edu/tqr>
- Gale, N. K., Heath, G., Cameron, E., Rashid, S., & Redwood, S. (2013). Using the framework method for the analysis of qualitative data in multi-disciplinary health research. *BMC Medical Research Methodology*, 13, 117-124.
doi:10.1186/1471-2288-13-117

- García, J. A. T., Skotnicka, A. G., & Zamora, D. T. (2015). The new technology-based firm profile required for a delimitation of its definition in empirical studies. *International Journal of Engineering Management and Economics*, 5(1-2), 114-128. doi:10.1504/IJEME.2015.069903
- Garfinkel, S. L. (2012). The cybersecurity risk. *Communications of the ACM*, 55(6), 29-32. doi:10.1145/2184319.2184330
- Geer, D. (2013). Resolved: The Internet is no place for critical infrastructure. *Communications of the ACM*, 56(6), 48-53. doi:10.1145/2461256.2461273
- Gentles, S. J., Charles, C., Ploeg, J., & McKibbin, K. (2015). Sampling in qualitative research: Insights from an overview of the methods literature. *The Qualitative Report*, 20(11), 1772-1789. Retrieved from <http://nsuworks.nova.edu/tqr/>
- Giboney, J. S., Proudfoot, J. G., Goel, S., & Valacich, J. S. (2016). The security expertise assessment measure (SEAM): Developing a scale for hacker expertise. *Computers & Security*, 60, 37-51. doi:10.1016/j.cose.2016.04.001
- Goldsborough, R. (2012). Preparing for the next emergency. *Teacher Librarian*, 40(2), 68. Retrieved from <http://www.teacherlibrarian.com>
- Gomes, R. (2015). Resilience and enterprise architecture in SMEs. *JISTEM-Journal of Information Systems and Technology Management*, 12, 525-540. doi:10.4301/S1807-17752015000300002
- Gootman, S. (2016). OPM hack: The most dangerous threat to the federal government today. *Journal of Applied Security Research*, 11(4), 517-525. doi:10.1080/19361610.2016.1211876

- Gordon, L. A., Loeb, M. P., & Zhou, L. (2016). Investing in cybersecurity: Insights from the Gordon-Loeb model. *Journal of Information Security, 7*, 49-59.
doi:10.4236/jis.2016.72004
- Gothberg, J., Reeves, P., Thurston, L., Applegate, B., Kohler, P., & Peterson, L. (2013). Is the medium really the message?: A comparison of face-to-face, telephone, and Internet focus group venues. *Journal of Ethnographic & Qualitative Research, 7*, 108-127. Retrieved from <http://www.jeqr.org/>
- Green, H. E. (2014). Use of theoretical and conceptual frameworks in qualitative research. *Nurse Researcher, 21*(6), 34-38. doi:10.7748/nr.21.6.34.e1252
- Grossman, J. (2013). The web won't be safe or secure until we break it. *Communications of the ACM, 56*(1), 68-72. doi:10.1145/2398356.2398373
- Grossoehme, D. H. (2014). Overview of qualitative research. *Journal of Health Care Chaplaincy, 20*, 109-122. doi:10.1080/08854726.2014.925660
- Gupta, P., Seetharaman, A., & Raj, J. R. (2013). The usage and adoption of cloud computing by small and medium businesses. *International Journal of Information Management, 33*, 861-874. doi:10.1016/j.ijinfomgt.2013.07.001
- Haichang, G., Wei, J., Fei, Y., & Licheng, M. (2013). A survey on the use of graphical passwords in security. *Journal of Software, 8*, 1678-1698.
doi:10.4304/jsw.8.7.1678-1698
- Haigh, T. (2014). We have never been digital. *Communications of the ACM, 57*(9), 24-28. doi:10.1145/2644148

- Hallett, R. E., & Barber, K. (2014). Ethnographic research in a cyber era. *Journal of Contemporary Ethnography*, 43, 306-330. doi:10.1177/0891241613497749
- Harris, M. A., & Patten, K. P. (2014). Mobile device security considerations for small- and medium-sized enterprise business mobility. *Information Management & Computer Security*, 22(1), 97-114. doi:10.1108/IMCS-03-2013-0019
- Harvey, L. (2015). Beyond member-checking: A dialogic approach to the research interview. *International Journal of Research & Method in Education*, 38, 23-38. doi:10.1080/1743727X.2014.914487
- Hayes, J., & Bodhani, A. (2013). Cyber security: Small firms under fire. *Engineering & Technology*, 8(6), 80-83. doi:10.1049/et.2013.0614
- Hazzan, O., & Nutov, L. (2014). Teaching and learning qualitative research ≈ Conducting qualitative research. *The Qualitative Report*, 19(24), 1-29. Retrieved from <http://nsuworks.nova.edu/tqr/>
- Heale, R., & Forbes, D. (2013). Understanding triangulation in research. *Evidence-Based Nursing*, 16, 98. doi:10.1136/eb-2013-101494
- Hong, J., & Reed, D. (2013). Passwords getting painful, computing still blissful. *Communications of the ACM*, 56(3), 10-11. doi:10.1145/2428556.2428560
- Hong, J. Y., Kang, I. J., Kim, S. B., & Park, C. J. (2013). Development of information security contents for learning hacking principles. *International Journal of Security & Its Applications*, 7, 137-146. doi:10.14257/ijisia.2013.7.6.14

- Houghton, C., Casey, D., Shaw, D., & Murphy, K. (2013). Rigour in qualitative case-study research. *Nurse Researcher*, 20(4), 12-17.
doi:10.7748/nr2013.03.20.4.12.e326
- Houghton, C., Murphy, K., Shaw, D., & Casey, D. (2015). Qualitative case study data analysis: An example from practice. *Nurse Researcher*, 22(5), 8-12.
doi:10.7748/nr.22.5.8.e1307
- Hu, Y.-H., & Scott, C. (2014). A case study of adopting security guidelines in undergraduate software engineering education. *Journal of Computer and Communications*, 2, 25-36. doi:10.4236/jcc.2014.214003
- Hua, J., & Bapna, S. (2013). The economic impact of cyber terrorism. *The Journal of Strategic Information Systems*, 22, 175-186. doi:10.1016/j.jsis.2012.10.004
- Huang, C. Y. (2013). Effective bot host detection based on network failure models. *Computer Networks*, 57, 514-525. doi:10.1016/j.comnet.2012.07.018
- Hyett, N., Kenny, A., & Dickson-Swift, V. (2014). Methodology or method?: A critical review of qualitative case study reports. *International Journal of Qualitative Studies on Health and Well-Being*, 9, 23606. doi:10.3402/qhw.v9.23606
- Hyman, P. (2013a). Augmented-reality glasses bring cloud security into sharp focus. *Communications of the ACM*, 56(6), 18-20. doi:10.1145/2461256.2461264
- Hyman, P. (2013b). Cybercrime: It's serious, but exactly how serious? *Communications of the ACM*, 56(3), 18-20. doi:10.1145/2428556.2428563
- Internet Crime Complaint Center (IC3). (2014). *2012 IC3 annual report*. Washington, DC. Retrieved from http://www.ic3.gov/media/annualreport/2012_IC3Report.pdf

- Irvine, A., Drew, P., & Sainsbury, R. (2012). Am I not answering your questions properly?: Clarification, adequacy and responsiveness in semi-structured telephone and face-to-face interviews. *Qualitative Research, 13*, 87-106.
doi:10.1177/1468794112439086
- Janghorban, R., Roudsari, R. L., & Taghipour, A. (2014). Skype interviewing: The new generation of online synchronous interview in qualitative research. *International Journal of Qualitative Studies on Health and Well-Being, 9*.
doi:10.3402/qhw.v9.24152
- Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences, 80*, 973-993.
doi:10.1016/j.jcss.2014.02
- Jansen, J., Veenstra, S., Zuurveen, R., & Stol, W. (2016). Guarding against online threats: Why entrepreneurs take protective measures. *Behaviour & Information Technology, 35*, 368-379. doi:10.1080/0144929X.2016.1160287
- Jansson, N. (2013). Organizational change as practice: A critical analysis. *Journal of Organizational Change Management, 26*, 1003-1019.
doi:10.1108/JOCM-09-2012-0152
- Jaradat, R. M., & Keating, C. B. (2014). Fragility of oil as a critical infrastructure problem. *International Journal of Critical Infrastructure Protection, 7*, 86-99.
doi:10.1016/j.ijcip.2014.04.005
- Julisch, K. (2013). Understanding and overcoming cyber security anti-patterns. *Computer Networks, 57*, 2206-2211. doi:10.1016/j.comnet.2012.11.023

- Keene, S. D. (2012). Emerging threats: Financial crime in the virtual world. *Journal of Money Laundering Control*, 15, 25-37. doi:10.1108/13685201211194718
- Kim, B. H., & Park, Y. G. (2013). Design and analysis of client control system using DNS control firewall. *International Journal of Smart Home*, 7(5), 135-143. doi:10.14257/ijsh.2013.7.5.14
- Kim, E. B. (2013). Information security awareness status of business college: Undergraduate students. *Information Security Journal: A Global Perspective*, 22(4), 171-179. doi:10.1080/19393555.2013.828803
- Kleemans, E., Soudijn, M., & Weenink, A. (2012). Organized crime, situational crime prevention and routine activity theory. *Trends in Organized Crime*, 15, 87-92. doi:10.1007/s12117-012-9173-1
- Koelsch, L. E. (2013). Reconceptualizing the member check interview. *International Journal of Qualitative Methods* 2013, 12(1), 168-179. Retrieved from <http://ejournals.library.ualberta.ca/index.php/IJQM>
- Kongnso, F. J. (2015). *Best practices to minimize data security breaches for increased business performance* (Doctoral dissertation). Available from ProQuest Dissertations & Theses Global (UMI No. 3739769)
- Kortjan, N., & Von Solms, R. (2014). A conceptual framework for cyber-security awareness and education in SA. *South African Computer Journal*, 52, 29-41. doi:10.18489/sacj.v52i0.201
- Kotz, D., Fu, K., Gunter, C., & Rubin, A. (2015). Security for mobile and cloud frontiers in healthcare. *Communications of the ACM*, 58(8), 21-23. doi:10.1145/2790830

- Kraemer-Mbula, E., Tang, P., & Rush, H. (2013). The cybercrime ecosystem: Online innovation in the shadows? *Technological Forecasting and Social Change*, *80*, 541-555. doi:10.1016/j.techfore.2012.07.002
- Kshetri, N. (2013). Cyber-victimization and cybersecurity in China. *Communications of the ACM*, *56*(4), 35-37. doi:10.1145/2436256.2436267
- Kuhn, T. (1970). *The structure of scientific revolutions*. Chicago, IL: University of Chicago Press.
- Kumar, N., & Chaudhary, P. (2014). Minimize cyber losses in cyber world through the optimization technique. *International Journal of Computer Applications (IJCA)*, *96*(20), 18-22. doi:10.5120/16910-6993
- Kutty, N. A., & Sreeramareddy, C. T. (2014). A cross-sectional online survey of compulsive internet use and mental health of young adults in Malaysia. *Journal of family & community medicine*, *21*(1), 23-28. doi:10.4103/2230-8229.128770
- Kuznetsov, V. D., Sinelnikov, V. M., & Alpert, S. N. (2015). Yakov Alpert: Sputnik-1 and the first satellite ionospheric experiment. *Advances in Space Research*, *55*, 2833-2839. doi:10.1016/j.asr.2015.02.033
- Laurie, B., & Doctorow, C. (2012). Computing: Secure the Internet. *Nature*, *491*, 325-326. doi:10.1038/491325a
- Layton, R., & Watters, P. A. (2014). A methodology for estimating the tangible cost of data breaches. *Journal of Information Security and Applications*, *19*, 321-330. doi:10.1016/j.jisa.2014.10.012 2214-2126

- Li, H. (2013). Design and implementation of a task manager of sensor network operating system. *Information Technology Journal*, 12, 6531-6536.
doi:10.3923/itj.2013.6531.6536
- Livshits, B., Bace, R., & Neville-Neil, G. (2013). Browser security: Appearances can be deceiving. *Communications of the ACM*, 56(1), 60-67.
doi:10.1145/2398356.2398372
- Lowe, M. (2014). Defending against cyber-criminals targeting business websites. *Network Security*, 8, 11-13. doi:10.1016/S1353-4858(14)70080-7
- Lunnay, B., Borlagdan, J., McNaughton, D., & Ward, P. (2014). Ethical use of social media to facilitate qualitative research. *Qualitative Health Research*, 25, 99-109.
doi:10.1177/1049732314549031
- MacEwan, N. (2013). A tricky situation: Deception in cyberspace. *Journal of Criminal Law*, 77, 417-432. doi:10.1350/jcla.2013.77.5.867
- Maduku, D. K., Mpinganjira, M., & Duh, H. (2016). Understanding mobile marketing adoption intention by South African SMEs: A multi-perspective framework. *International Journal of Information Management*, 36, 711-723.
doi:10.1016/j.ijinfomgt.2016.04.018
- Malik, F. (2013). Application of data mining in changing times and its role in future. *Indian Journal of Commerce and Management Studies*, 4(1), 73-77. Retrieved from <http://www.scholarshub.net/ijcms.html>
- Mandal, K. K., & Chatterjee, D. (2015). Insider threat mitigation in cloud computing. *International Journal of Computer Applications*, 120, 7-11.

doi:10.5120/21341-4352

- Manning, J. (2014). A constitutive approach to interpersonal communication studies. *Communication Studies*, 65, 432-440. doi:10.1080/10510974.2014.927294
- Marshall, B., Cardon, P., Poddar, A., & Fontenot, R. (2013). Does sample size matter in qualitative research?: A review of qualitative interviews in IS research. *The Journal of Computer Information Systems*, 54(1), 11-22. Retrieved from <http://www.iacis.org/jcis/jcis.php>
- Marshall, C., & Rossman, G. B. (2016). *Designing qualitative research* (6th ed.). Thousand Oaks, CA: Sage.
- Maughan, D., Balenson, D., Lindqvist, U., & Tudor, Z. (2015). Government-funded R&D to drive cybersecurity technologies. *IT Professional*, 17(4), 62-65. doi:10.1109/MITP.2015.70
- Mayoh, J., & Onwuegbuzie, A. J. (2015). Toward a conceptualization of mixed methods phenomenological research. *Journal of Mixed Methods Research*, 9, 91-107. doi:10.1177/1558689813505358
- McAreavey, R., & Das, C. (2013). A delicate balancing act: Negotiating with gatekeepers for ethical research when researching minority communities. *International Journal of Qualitative Methods*, 12, 113-131. Retrieved from <http://ejournals.library.ualberta.ca/index.php/IJQM>
- Melbourne Regional Chamber of East Central Florida. (2016). *Melbourne Regional Chamber of East Central Florida*. Melbourne, FL. Retrieved from <http://www.melbourneregionalchamber.com/>

- Mijnhardt, F., Baars, T., & Spruit, M. (2016). Organizational characteristics influencing SME information security maturity. *Journal of Computer Information Systems*, 56, 106-115. doi:10.1080/08874417.2016.1117369
- Miles, K. J. (2013). *Exploring factors required for small business success in the 21st century* (Doctoral Dissertations). Available from ProQuest Digital Dissertations and Theses database. (Order No. 3560237)
- Mishra, S., Caputo, D. J., Leone, G. J., Kohun, F. G., & Draus, P. J. (2014). The role of awareness and communications in information security management: A health care information systems perspective. *International Journal of Management & Information Systems (Online)*, 18, 139-138. doi:10.19030/ijmis.v18i2.8495
- Mone, G. (2013). Future-proof encryption. *Communications of the ACM*, 56(11), 12-14. doi:10.1145/2524713.2524718
- Morgan, D. L. (2014). Pragmatism as a paradigm for social research. *Qualitative Inquiry*, 20, 1045-1053. doi:10.1177/1077800413513733
- Morse, A. L., & McEvoy, C. D. (2014). Qualitative research in sport management: Case study as a methodological approach. *The Qualitative Report*, 19(17), 1-13. Retrieved from <http://nsuworks.nova.edu/tqr/>
- Murthy, D. (2013). Ethnographic research 2.0: The potentialities of emergent digital technologies for qualitative organizational research. *Journal of Organizational Ethnography*, 2, 23-36. doi:10.1108/JOE-01-2012-0008

- Nagunwa, T. (2014). Behind identity theft and fraud in cyberspace: the current landscape of phishing vectors. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, 3, 72-83. doi:10.17781/P001287
- National Cyber Security Alliance [NCSA]. (2015). *3 reasons hackers love your small business infographic*. Retrieved from <https://www.staysafeonline.org/ncsam/resources/3-reasons-hackers-love-your-small-business-infographic>
- National Institute of Standards and Technology [NIST]. (2015a). *Cybersecurity framework*. Gaithersburg, MD. Retrieved from <http://www.nist.gov/cyberframework/index.cfm>
- National Institute of Standards and Technology [NIST]. (2015b). *Framework for improving critical infrastructure cybersecurity, version 1.0*. Gaithersburg, MD. Retrieved from <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>
- National Institutes of Health [NIH]. (2012). *National Institutes of Health (NIH) policies and procedures for promoting scientific integrity*. Bethesda, MD. Retrieved from <http://www.nih.gov>
- Nishimura, A., Carey, J., Erwin, P. J., Tilburt, J. C., Murad, M. H., & McCormick, J. B. (2013). Improving understanding in the research informed consent process: A systematic review of 54 interventions tested in randomized control trials. *BMC Medical Ethics*, 14, 1-28. doi:10.1186/1472-6939-14-28
- Njenga, K., & Jordaan, P. (2016). We want to do it our way: The neutralization approach to managing information systems security by small businesses. *The African*

- Journal of Information Systems*, 8(1), 3. 42-63. Retrieved from <http://digitalcommons.kennesaw.edu/ajis/>
- Noble, H., & Smith, J. (2015). Issues of validity and reliability in qualitative research. *Evidence Based Nursing*, 18(2), 34-35. doi:10.1136/eb-2015-102054
- Nottingham, S., & Henning, J. (2014). Feedback in clinical education, part I: Characteristics of feedback provided by approved clinical instructors. *Journal of Athletic Training*, 49, 49-57. doi:10.4085/1062-6050-48.6.14
- Onwuegbuzie, A. J., & Byers, V. T. (2014). An exemplar for combining the collection, analysis, and interpretation of verbal and nonverbal data in qualitative research. *International Journal of Education*, 6, 183-246. doi:10.5296/ije.v6i1.4399
- O'Reilly, M., & Parker, N. (2013). Unsatisfactory saturation: A critical exploration of the notion of saturated sample sizes in qualitative research. *Qualitative Research Journal*, 13(2), 1-8. doi:10.1177/1468794112446106
- Owen, G. T. (2014). Qualitative methods in higher education policy analysis: Using interviews and document analysis. *The Qualitative Report*, 19(26), 1-19. Retrieved from <http://nsuworks.nova.edu/tqr/>
- Pacho, T. O. (2015). Exploring participants' experiences using case study. *International Journal of Humanities and Social Science*, 5(4), 44-53. Retrieved from <http://www.ijhssnet.com/>
- Palinkas, L. A. (2014). Qualitative and mixed methods in mental health services and implementation research. *Journal of Clinical Child & Adolescent Psychology*, 43, 851-861. doi:10.1080/15374416.2014.910791

- Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2013). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Adm Policy Ment Health, 42*, 533-544. doi:10.1007/s10488-013-0528-y
- Pattinson, S., & Preece, D. (2014). Communities of practice, knowledge acquisition and innovation: A case study of science-based SMEs. *Journal of Knowledge Management, 18*, 107-120. doi:10.1108/JKM-05-2013-0168
- Patton, M. Q. (2015). *Qualitative research & evaluation methods: Integrating theory and practice*. (4th ed.). Thousand Oaks, CA: Sage.
- Paulsen, C., McDuffie, E., Newhouse, W., & Toth, P. (2012). NICE: Creating a cybersecurity workforce and aware public. *IEEE Security & Privacy, 10*(3), 76-79. doi:10.1109/MSP.2012.73
- 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
- Perry, S. L. (2013). Using ethnography to monitor the community health implications of onshore unconventional oil and gas developments: Examples from Pennsylvania's Marcellus Shale. *New Solutions, 23*, 33-53. doi:10.2190/NS.23.1.d
- Petty, N. J., Thomson, O. P., & Stew, G. (2012). Ready for a paradigm shift? part 2: Introducing qualitative research methodologies and methods. *Manual Therapy, 17*, 378-384. doi:10.1016/j.math.2012.03.004

- Piggin, R. (2016). Cyber security trends: What should keep CEOs awake at night. *International Journal of Critical Infrastructure Protection*, 13, 36-38.
doi:10.1016/j.ijcip.2016.04.001
- Poni, M. (2014). Research paradigms in education. *Journal of Educational and Social Research*, 4, 407-414. doi:10.5901/jesr.2014.v4n1p407
- Pouvreau, D. (2014). On the history of Ludwig von Bertalanffy's "general systemology," and on its relationship to cybernetics-part II: Contexts and developments of the systemological hermeneutics instigated by von Bertalanffy. *International Journal of General Systems*, 43, 172-245. doi:10.1080/03081079.2014.883743
- Prayudi, Y., & Yusirwan, S. (2015). The recognize of malware characteristics through static and dynamic analysis approach as an effort to prevent cybercrime activities. *Journal of Theoretical & Applied Information Technology*, 77, 438-445.
Retrieved from <http://www.jatit.org>
- Protecting small businesses against emerging and complex cyber-attacks: Hearing before the subcommittee on health and technology of the committee on small business, House of Representatives, 113th Cong. 1. (2013). Retrieved from <https://www.gpo.gov/fdsys/pkg/CHRG-113hrg80172/pdf/CHRG-113hrg80172.pdf>
- Querstret, D., & Robinson, O. C. (2013). Person, persona and personality modification: An in-depth qualitative exploration of quantitative findings. *Qualitative Research in Psychology*, 10, 140-159. doi:10.1080/14780887.2011.586450

- Rabai, L. B. A., Jouini, M., Aissa, A. B., & Mili, A. (2013). A cybersecurity model in cloud computing environments. *Journal of King Saud University-Computer and Information Sciences*, 25, 63-75. doi:10.1016/j.jksuci.2012.06.002
- Raiyn, J. (2014). A survey of cyber attack detection strategies. *International Journal of Security and Its Applications*, 8(1), 247-256. doi:10.14257/ijcia.2014.8.1.23
- Ramayah, T., Ling, N. S., Taghizadeh, S. K., & Rahman, S. A. (2015). Factors influencing SMEs website continuance intention in Malaysia. *Telematics and Informatics*, 33(1), 150-164. doi:10.1016/j.tele.2015.06.007
- Rashid, A., & Parvez, J. (2014). Mobile cloud computing: A survey of emerging issues and future trends. *International Journal of Engineering Science and Technology*, 6, 295-300. Retrieved from <http://www.ijest.info>
- Raza, S., Wallgren, L., & Voigt, T. (2013). SVELTE: Real-time intrusion detection in the Internet of things. *Ad hoc networks*, 11, 2661-2674. doi:10.1016/j.adhoc.2013.04.014
- Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies*, 38(1-2), 4-37. doi:10.1080/01402390.2014.977382
- Robinson, O. C. (2014). Sampling in interview-based qualitative research: A theoretical and practical guide. *Qualitative Research in Psychology*, 11, 25-41. doi:10.1080/14780887.2013.801543
- Rossetto, K. R. (2014). Qualitative research interviews: Assessing the therapeutic value and challenges. *Journal of Social and Personal Relationships*, 31, 482-489. doi:10.1177/0265407514522892

- Salman, A., Saad, S., & Ali, M. N. S. (2013). Dealing with ethical issues among Internet users: Do we need legal enforcement? *Asian Social Science*, 9(8), 3-8.
doi:10.5539/ass.v9n8p3
- Sangster-Gormley, E. (2013). How case-study research can help to explain implementation of the nurse practitioner role. *Nurse Researcher*, 20(4), 6-11.
doi:10.7748/nr2013.03.20.4.6.e291
- Sargeant, J. (2012). Qualitative research part II: Participants, analysis, and quality assurance. *Journal of Graduate Medical Education*, 4, 1-3. doi:10.4300/JGME-D-11-00307.1
- Saunders, B., Kitzinger, J., & Kitzinger, C. (2014). Participant anonymity in the Internet age: From theory to practice. *Qualitative Research in Psychology*, 12, 125-137.
doi:10.1080/14780887.2014.948697
- Scheibe, M., Reichelt, J., Bellmann, M., & Kirch, W. (2015). Acceptance factors of mobile apps for diabetes by patients aged 50 or older: A qualitative study. *Medicine 2.0*, 4(1), e1-e13. doi:10.2196/med20.3912
- Schneck, P. (2014, October 24). *Department of Homeland Security (DHS) - improving cybersecurity for small and medium-sized businesses*. [Blog post]. Retrieved from <http://www.dhs.gov/blog/2014/10/24/improving-cybersecurity-small-and-medium-sized-businesses>
- Shackelford, S., Fort, T. L., & Prenkert, J. D. (2015). How businesses can promote cyber peace. *University of Pennsylvania Journal of International Law*, Kelley School of Business Research Paper No. 2014-27. Retrieved from <http://www.pennjil.com/>

- Shahzad, A., Hussain, M., & Khan, M. N. A. (2013). Protecting from zero-day malware attacks. *Middle East Journal of Scientific Research*, 17, 455-464.
doi:10.5829/idosi.mejsr.2013.17.04.12159
- Sheldon, F. T., & McDonald, J. T. (2012). Introduction to the special issue on cyber security and management. *Information Systems & E-Business Management*, 10, 429-431. doi:10.1007/s10257-012-0204-x
- Sheppard, B., Crannell, M., & Moulton, J. (2013). Cyber first aid: Proactive risk management and decision-making. *Environment Systems & Decisions*, 33, 530-535. doi:10.1007/s10669-013-9474-1
- Shin, D., & Konrad, A. M. (2017). Causality between high-performance work systems and organizational performance. *Journal of Management*, 43, 973-997.
doi:10.1177/0149206314544746
- Sigholm, J. (2013). Non-state actors in cyberspace operations. *Journal of Military Studies*, 4(1), 1-37. Retrieved from <http://ojs.tsv.fi/index.php/jms/index>
- Singh, J. (2014). Comprehensive solution to mitigate the cyber-attacks in cloud computing. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, 3, 84-92. doi:10.17781/p001294
- Smith, J., & Noble, H. (2014). Bias in research. *Evidence-Based Nursing*, 17, 100-101.
doi:10.1136/eb-2014-101946
- Snelgrove, S. R. (2014). Conducting qualitative longitudinal research using interpretative phenomenological analysis. *Nurse Researcher*, 22(1), 20-25. Retrieved from <http://rcnpublishing.com/journal/nr>

- Son, H. J., & Jeong, S. (2013). A research on security awareness and countermeasures for the single server. *International Journal of Security & Its Applications*, 7(6), 31-41. doi:10.14257/ijisia.2013.7.6.04
- Sotiriadou, P., Brouwers, J., & Le, T. A. (2014). Choosing a qualitative data analysis tool: A comparison of NVivo and leximancer. *Annals of Leisure Research*, 17, 218-234. doi:10.1080/11745398.2014.902292
- Space Coast Score. (2016, June 20). *Space coast score*. Retrieved from <https://spacecoast.score.org/>
- Srinidhi, B., Yan, J., & Tayi, G. K. (2015). Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors. *Decision Support Systems*, 75, 49-62. doi:10.1016/j.dss.2015.04.011
- Steinmetz, K. F. (2014). Craft(y)ness. *British Journal of Criminology*, 55, 125-145. doi:10.1093/bjc/azu061
- Sultan, N. (2014). Making use of cloud computing for healthcare provision: Opportunities and challenges. *International Journal of Information Management*, 34(2), 177-184. doi:10.1016/j.ijinfomgt.2013.12.011
- Symantec Corporation. (2013). *Internet security threat report (ISTR) 2013* (Volume 18). Mountain View, CA: Author. Retrieved from http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf
- Symantec Corporation. (2015). *Internet security threat report (ISTR) 2015* (Volume 20). Mountain View, CA: Author. Retrieved from <https://www4.symantec.com/>

mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf

Symantec Corporation. (2016). *Internet security threat report (ISTR) 2016* (Volume 21).

Mountain View, CA: Author. Retrieved from <https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf>

Taddeo, M. (2013). Cyber security and individual rights, striking the right balance ethics.

Philosophy & Technology, 26, 353-356. doi:10.1007/s13347-013-0140-9

Tchakounté, F. (2014). Permission-based malware detection mechanisms on android:

Analysis and perspectives. *Journal of Computer Science*, 1(2), 63-77. Retrieved from <http://thescipub.com/journals/jcs>

The White House, United States Government. (2014). *Foreign policy: Cyber security*.

Washington, DC. Retrieved from <https://www.whitehouse.gov/issues/foreign-policy/cybersecurity>

The White House, United States Government. (2015a). *Executive order: Executive order*

-- *improving critical infrastructure cybersecurity*. Washington, DC. Retrieved from <https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>

The White House, United States Government. (2015b). *Foreign policy. The*

comprehensive national cybersecurity initiative. Washington, DC. Retrieved from <https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative>

- Tong, A., Chapman, J. R., Israni, A., Gordon, E. J., & Craig, J. C. (2013). Qualitative research in organ transplantation: Recent contributions to clinical care and policy. *American Journal of Transplantation, 13*, 1390-1399. doi:10.1111/ajt.12239
- Trafimow, D. (2014). Considering quantitative and qualitative issues together. *Qualitative Research in Psychology, 11*, 15-24. doi:10.1080/14780887.2012.743202
- Tsang, E. W. (2014). Case studies and generalization in information systems research: A critical realist perspective. *The Journal of Strategic Information Systems, 23*, 174-186. doi:10.1016/j.jsis.2013.09.002
- Tuohy, D., Cooney, A., Dowling, M., Murphy, K., & Sixsmith, J. (2013). An overview of interpretive phenomenology as a research methodology. *Nurse Researcher, 20*(6), 17-20. Retrieved from <http://journals.rcni.com/journal/nr>
- United States Census Bureau. (2013). *Statistics of U.S. businesses*. [2013 SUSB annual data tables by establishment industry]. Washington, DC. Retrieved from <http://www.census.gov/programs-surveys/susb.html>
- United States Census Bureau. (2015). *QuickFacts, Melbourne city, Florida*. Washington, DC. Retrieved from <http://www.census.gov/quickfacts/table/PST045215/1243975>
- United States Department of Health & Human Services [DHHS]. (1979, April). Ethical principles and guidelines for the protection of human subjects of research. *Human Subjects Research (45 CFR 46). The Belmont Report*. Washington, DC. Retrieved from <http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html>

United States Department of Homeland Security [DHS]. (2015a). *Cybersecurity tips*.

Washington, DC. Retrieved from <http://www.dhs.gov/cybersecurity-tips>

United States Department of Homeland Security [DHS]. (2015b). *History*. Washington,

DC. Retrieved from <http://www.dhs.gov/history>

United States Department of Homeland Security [DHS]. (2015c). *National strategy to*

secure cyberspace. Washington, DC. Retrieved from [http://www.dhs.gov/](http://www.dhs.gov/national-strategy-secure-cyberspace)

[national-strategy-secure-cyberspace](http://www.dhs.gov/national-strategy-secure-cyberspace)

United States Government Accountability Office [GAO]. (2013). *GAO-13-187,*

cybersecurity – United States government accountability office report to

congressional addresses. Washington, DC. Retrieved from [http://gao.gov/](http://gao.gov/assets/660/652170.pdf)

[assets/660/652170.pdf](http://gao.gov/assets/660/652170.pdf)

United States Government Accountability Office [GAO]. (2015). *Key issues:*

Cybersecurity. Washington, DC. Retrieved from [http://www.gao.gov/](http://www.gao.gov/key_issues/cybersecurity/issue_summary)

[key_issues/cybersecurity/issue_summary](http://www.gao.gov/key_issues/cybersecurity/issue_summary)

United States Securities and Exchange Commission [SEC]. (2015). *The need for greater*

focus on the cybersecurity challenges facing small and midsize businesses.

Washington, DC. Retrieved from [https://www.sec.gov/news/statement/](https://www.sec.gov/news/statement/cybersecurity-challenges-for-small-midsize-businesses.html)

[cybersecurity-challenges-for-small-midsize-businesses.html](https://www.sec.gov/news/statement/cybersecurity-challenges-for-small-midsize-businesses.html)

United States Small Business Administration [SBA]. (2012). *Frequently asked questions*

about small business. Washington, DC. Retrieved from [https://www.sba.gov/](https://www.sba.gov/sites/default/files/FAQ_Sept_2012.pdf)

[sites/default/files/FAQ_Sept_2012.pdf](https://www.sba.gov/sites/default/files/FAQ_Sept_2012.pdf)

- United States Small Business Administration [SBA]. (2014). *Do small businesses need to worry about cyber security?* Washington, DC. Retrieved from <https://www.sba.gov/blogs/do-small-businesses-need-worry-about-cyber-security>
- United States Small Business Administration [SBA]. (2015). *Starting & managing business, cybersecurity.* Washington, DC. Retrieved from <https://www.sba.gov/navigation-structure/cybersecurity>
- United States Small Business Administration [SBA]. (2016a). *Online business law.* Washington, DC. Retrieved from <https://www.sba.gov/managing-business/business-law-regulations/industry-laws-regulations/online-business-law>
- United States Small Business Administration [SBA]. (2016b). *Resource guide for small businesses.* Washington, DC. Retrieved from https://www.sba.gov/sites/default/files/files/resourceguide_3109.pdf
- Vaismoradi, M., Turunen, H., & Bondas, T. (2013). Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study. *Nursing and Health Sciences, 15*, 398-405. doi:10.1111/nhs.12048
- Valizadeh, S., Dadkhah, B., Mohammadi, E., & Hassankhani, H. (2014). The perception of trauma patients from social support in adjustment to lower-limb amputation: A qualitative study. *Indian Journal of Palliative Care, 20*, 229-238. doi:10.4103/0973-1075.138401
- Verbano, C., & Venturini, K. (2013). Managing risks in SMEs: A literature review and research agenda. *Journal of technology management & innovation, 8*(3), 186-197. doi:10.4067/S0718-27242013000400017

- von Bertalanffy, L. (1968). *General systems theory: Foundations, development, application* (Rev. ed.). New York, NY: George Braziller.
- Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97-102. doi:10.1016/j.cose.2013.04.004
- Wahyuni, D. (2012). The research design maze: Understanding paradigms, cases, methods and methodologies. *Journal of Applied Management Accounting Research, 10*(1), 69-80. Retrieved from <http://cmaweblines.org/index.php>
- Walker-Osborn, C., & McLeod, B. (2015). Getting tough on cyber crime. *ITNOW, 57*(2), 32-33. doi:10.1093/itnow/bwv042
- Wang, W., & Lu, Z. (2013). Cyber security in the smart grid: Survey and challenges. *Computer Networks, 57*, 1344-1371. doi:10.1016/j.comnet.2012.12.017
- Weber, R. M., & Horn, B. D. (2017). Breaking bad security vulnerabilities. *Journal of Financial Service Professionals, 71*, 50-54. Retrieved from http://www.financialpro.org/pubs/journal_index.cfm
- Wen, J., Ma, J., Huang, R., Jin, Q., Chen, J., Huang, B., & Zhong, N. (2014). A malicious behavior analysis based cyber-I birth. *Journal of Intelligent Manufacturing, 25*, 147-155. doi:10.1007/s10845-012-0681-2
- Whaiduzzaman, M., Sookhak, M., Gani, A., & Buyya, R. (2014). A survey on vehicular cloud computing. *Journal of Network and Computer Applications, 40*, 325-344. doi:10.1016/j.jnca.2013.08.004
- Whitty, M., Doodson, J., Creese, S., & Hodges, D. (2015). Individual differences in cyber security behaviors: An examination of who is sharing passwords.

Cyberpsychology, Behavior and Social Networking, 18, 3-7. doi:10.1089/cyber.2014.0179

Wickens, C. D., Clegg, B. A., Vieane, A. Z., & Sebok, A. L. (2015). Complacency and automation bias in the use of imperfect automation. *Human Factors*, 57, 728-739. doi:10.1177/0018720815581940

Wolf, L. E., Patel, M. J., Williams Tarver, B. A., Austin, J. L., Dame, L. A., & Beskow, L. M. (2015). Certificates of confidentiality: Protecting human subject research data in law and practice. *The Journal of Law, Medicine & Ethics*, 43, 594-609. Retrieved from <https://www.aslme.org/Publications>

Wolfswinkel, J. F., Furtmueller, E., & Wilderom, C. P. M. (2013). Using grounded theory as a method for rigorously reviewing literature. *European Journal of Information Systems*, 22, 45-55. doi:10.1057/ejis.2011.51

Xu, Z., Hu, Q., & Zhang, C. (2013). Why computer talents become computer hackers. *Communications of the ACM*, 56(4), 64-74. doi:10.1145/2436256.2436272

Yager, Z., Diedrichs, P. C., & Drummond, M. (2013). Understanding the role of gender in body image research settings: Participant gender preferences for researchers and co-participants in interviews, focus groups and interventions. *Body Image*, 10, 574-582. doi:10.1016/j.bodyim.2013.06.004

Ye, N., Aranda, B. M., & Hurley, P. (2013). System impact characteristics of cyber services, security mechanisms, and attacks with implications in cyber system survivability. *Information Knowledge Systems Management*, 12, 75-95. doi:10.3233/IKS-130217

- Yeboah-Boateng, E. O. (2013). Of social engineers & corporate espionage agents: How prepared are SMEs in developing economies? *Journal of Electronics & Communications Engineering Research*, 1(3), 14-22. Retrieved from <http://www.questjournals.org/>
- Yelland, M. (2013). Fraud in mobile networks. *Computer Fraud & Security*, 3, 5-9. doi:10.1016/S1361-3723(13)70027-7
- Yilmaz, K. (2013). Comparison of quantitative and qualitative research traditions: Epistemological, theoretical, and methodological differences. *European Journal of Education*, 48, 311-325. doi:10.1111/ejed.12014
- Yin, R. K. (2013). Validity and generalization in future case study evaluations. *Evaluation*, 19, 312-332. doi:10.1177/1356389013497081
- Yin, R. K. (2014). *Case study research: Design and methods* (5th ed.). Thousand Oaks, CA: Sage.
- Young, W., & Leveson, N. G. (2014). An integrated approach to safety and security based on systems theory. *Communications of the ACM*, 57(2), 31-35. doi:10.1145/2556938
- Zamawe, F. C. (2015). The implication of using NVivo software in qualitative data analysis: Evidence-based reflections. *Malawi Medical Journal*, 27, 13-15. doi:10.4314/mmj.v27i1.4
- Zhang, X., Tsang, A., Yue, W. T., & Chau, M. (2015). The classification of hackers by knowledge exchange behaviors. *Information Systems Frontiers*, 17, 1239-1251. doi:10.1007/s10796-105-9567-0

Zhao, J. J., & Zhao, S. Y. (2012). Retail E-commerce security status among fortune 500 corporations. *Journal of Education for Business*, 87, 136-144.

doi:10.1080/08832323.2011.582191

Appendix A: SME Owner's Cyber Security Strategies Interview Questions

Interview Questions

1. What successful strategies do you use to protect your infrastructure from cyber attacks?
2. What successful strategies do you use for preventing, detecting, and responding to cyber attack incidents?
3. How do you assess your information technology security risks?
4. What employee training strategies do you use for security procedures with Internet devices?
5. What risk management strategies do you use to identify and evaluate cyber attack risks?
6. What is your cyber attack contingency plan?
7. What effective strategies would you recommend to other SME owners to prevent a cyber attack?
8. What additional information on cyber security strategies would you like to provide or expound upon before ending the interview?

Appendix B: Participant Recruitment Letter

Date:

Subject: Request to Participate in a Research Study

Dear (Recipient):

I am a student at Walden University pursuing a Doctor of Business Administration (DBA) degree. I am conducting a research study of cyber security for small and medium-size enterprise (SME) owners in Melbourne, FL. The title of my study is Effective Cyber Security Strategies for Small Businesses. I am exploring SME owners' decisions regarding computer security strategies and practices, and would like to interview SME owners who meet all of the following criteria:

1. licensed to operate a retail business in Melbourne, Brevard County, Florida;
2. employing between one and 249 personnel;
3. have an annual gross revenue of under \$10 million;
4. have successfully implemented cyber security strategies.

Face-to-face interviews with small business owners may provide helpful insight and understanding to increase knowledge and mitigate cyber attacks. I estimate your time commitment to fully participate in this study will range from 40 to 60 minutes. Upon completion of the study, I will share the research findings with study participants, small business owners, and with fellow university researchers. If you meet the above criteria and are interested in participating in this study, please contact me within 5 days via e-mail. Attached is a consent form further explaining the study and requesting your signature for consent to participate and audio record the interview.

I look forward to hearing from you soon.

Sincerely,

Encl. (1)

Appendix C: Interview Protocol

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

Type of Interview: _____

Date: _____

Place: _____

Interviewer: _____

Interviewee: _____

Position Title of Interviewee: _____

[Describe the project; explain to the interviewee about the (a) purpose of the study, (b) multiple sources of data collection, (c) data confidentiality, and (d) completion of the interview in less than one hour.]

[Provide the interviewee with contact information.]

[Request the SME owner provide copies of any additional relevant company documentation he/she would like to share.]

[Remind the interviewee of the consent form to participate in the study and to audio record the interview (provide copy if required).]

[Turn on the digital audio recorder and test device for functionality.]

Interview Questions:

1. What successful strategies do you use to protect your infrastructure from cyber attacks?
2. What successful strategies do you use for preventing, detecting, and responding to cyber attack incidents?

3. How do you assess your information technology security risks?
4. What employee training strategies do you use for security procedures with Internet devices?
5. What risk management strategies do you use to identify and evaluate cyber attack risks?
6. What is your cyber attack contingency plan?
7. What effective strategies would you recommend to other SME owners to prevent a cyber attack?
8. What additional information on cyber security strategies would you like to provide or expound upon before ending the interview?

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

Appendix D: Study Participant Thank-You Note

Dear Study Participant CS-X (1, 2, 3, 4),

Thank you for the opportunity of meeting with me and providing honest information, which will significantly impact the results of my doctoral study.

I sincerely appreciate the information you have provided and reiterate its confidentiality. As we discussed at the conclusion of our interview, you will receive an email with the transcribed interpretative file within the next 24 hours.

It was a pleasure meeting you and learning about your proactive efforts to ensure effective cyber security strategies.

Sincerely,

Appendix E: Study Participant Member Checking

Dear Study Participant CS-X (1, 2, 3, 4),

As we discussed at the conclusion of your interview, attached is the data interpretation file from the interview session. Should you concur in the data interpretation file, no response is necessary. Nonreceipt of a reply within 2 days provides concurrence.

Should you disagree with my interpretation of any of your responses, please provide corrections as necessary to me within the next 2 days via email. You may expect a revised data interpretation file incorporating your comments within 1 day. Should you concur in the revised data interpretation file, no response is necessary. Nonreceipt of a reply within 2 days provides concurrence.

If you have questions, please feel free to contact me via email.

Sincerely,

Encl (1)

Appendix F: Study Participant Comments of Data Interpretation File

Dear Study Participant CS-X (1, 2, 3, 4),

As we discussed at the conclusion of your interview, member checking is a critical element of doctoral studies. I have reviewed and incorporated your comments. Attached is the revised data interpretation file for your review and concurrence. Should you concur in the revised data interpretation file, no response is necessary. Nonreceipt of a reply within 2 days provides concurrence.

Should you disagree with my interpretation of any of your responses, please provide additional comments to me via email within 2 days. You may expect a revised data interpretation file incorporating your comments within 1 day. Should you concur in the revised data interpretation file, no response is necessary. Nonreceipt of a reply within 2 days provides concurrence.

If you have questions, please feel free to contact me via email.

Sincerely,

Encl (1)

Appendix G: Study Participant Interpretative Responses File

Dear Study Participant CS-X (1, 2, 3, 4),

As we discussed at the conclusion of your interview, attached is the transcribed interpretative file for your review regarding content. Please provide any comments to me via e-mail within the next 24 hours.

Question 1. What successful strategies do you use to protect your infrastructure from cyber attacks?

Response 1.

Question 2. What successful strategies do you use for preventing, detecting, and responding to cyber attack incidents?

Response 2.

Question 3. How do you assess your information technology security risks?

Response 3.

Question 4. What employee training strategies do you use for security procedures with Internet devices?

Response 4.

Question 5. What risk management strategies do you use to identify and evaluate cyber attack risks?

Response 5.

Question 6. What is your cyber attack contingency plan?

Response 6.

Question 7. What effective strategies would you recommend to other SME owners to prevent a cyber attack?

Response 7.

Question 8. What additional information on cyber security strategies would you like to provide or expound upon before ending the interview?

Response 8.