2017

Cyber-Security Policy Decisions in Small Businesses

Joanna Patterson
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Joanna Patterson

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. Elisabeth Musil, Committee Chairperson, Doctor of Business Administration Faculty

Dr. Alexandre Lazo, Committee Member, Doctor of Business Administration Faculty

Dr. Scott Burrus, University Reviewer, Doctor of Business Administration Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2017

Abstract

Cyber-Security Policy Decisions in Small Businesses

by

Joanna Patterson

MBA, Saint Leo University, 2013

BS, Bellevue University, 2011

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

November 2017

Abstract

Cyber-attacks against small businesses are on the rise yet small business owners often lack effective strategies to avoid these attacks. The purpose of this qualitative multiple case study was to explore the strategies small business owners use to make cyber-security decisions. Bertalanffy's general systems theory provided the conceptual framework for this study. A purposive sample of 10 small business owners participated in the interview process and shared their decision-making methodologies and influencers. The small business owners were vetted to ensure their strategies were effective through a series of qualification questions. The intent of the research question and corresponding interview questions was to identify strategies that successful small business owners use to make cyber-security decisions. Data analysis consisted of coding keywords, phrases, and sentences from semi structured interviews as well as document analysis. The following themes emerged: government requirements, peer influence, budgetary constraints, commercial standards, and lack of employee involvement. According to the participants, budgetary constraints and peer influence were the most influential factors when making decisions regarding cyber-security strategies. Through exposing small business owners to proven strategies, the implications for social change include a reduction of their small business operating costs and assistance with compliance activities.

Cyber-Security Policy Decisions in Small Businesses

by

Joanna Patterson

MBA, Saint Leo University, 2013

BS, Bellevue University, 2011

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

November 2017

Dedication

If we all limited ourselves to what others thought of our abilities the world would be a shell of what it is today. To Nina (from the house of Nina’s), thank you for being an unwavering light in the dark. Thank you for never giving up and always believing I could be more. To my mom, thank you for giving me every opportunity you possibly could. I never took it for granted, and I hope it shows.

Acknowledgements

To my professors, especially my committee chair, Dr. Elisabeth Musil, thank you for your guidance, wisdom, and tolerance. I hope to one day pay it forward. Thank you to my second committee member, Dr. Alexandre Lazo, and my university research reviewer, Dr. Scott Burrus, for their contributions made to my study. I would also like to thank all the participants who participated, ultimately making this study possible. Lastly, I am thankful for my co-workers, family, and friends who gave me encouragement and strength to complete my doctoral degree. Never underestimate the words of encouragement that you give to someone.

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

The advent of technology comes with an increasingly unstable and changing landscape. Cyber-security threats continue to evolve and reinvent themselves making cyber-attacks a concern for anyone utilizing technology (Dinicu, 2014). One particularly vulnerable group is small businesses. Small businesses have become an increasingly popular target for cyber-attacks for several reasons. Specifically, small business owners lack a cyber-security infrastructure capable of keeping up with cyber-security threats. Furthermore, hackers perceive small businesses as gateways to large businesses, including government entities, due to established business relationships (Shackelford, 2016).

While small business owners have struggled in years past to keep up with combating cyber-security threats, it is not immediately clear what small business owners must prioritize to maintain some degree of sanctity. What is clear is that small business owners lack effective strategies to make informed decisions to protect the business from cyber-attacks. In fact, an estimated 80% of small businesses reported not having cyber-security policies in place (Shackelford, 2016). This qualitative case study will explore what strategies small business owners can adopt when making decisions regarding protecting themselves from cyber-attacks.

Background of the Problem

In this age of digital technology, no business or government entity is safe from cyber-attacks. Cyber criminals do not target organizations based on size, rather the information or access held by that organization. The increasing adoption of information technology for business activities has increased the number of vulnerabilities and threats faced by businesses. Scholars and business entities alike have increased the number of resources devoted to the protection of these assets (Sen & Borle, 2015).

The U.S. Secret Service and Verizon have reported a spike in cyber crimes against small businesses that coincide with the increased use of technology (Wright, 2011). Small business owners are increasingly adopting technology related activities such as electronic commerce, which leaves them susceptible to cyber crimes (Rahman & Lackey, 2013). While crimes against small businesses increase, resources and strategic direction are minimal. A limited number of studies currently address why small business owners do not implement adequate cyber-security strategies.

Problem Statement

Cyber-security attacks explicitly aimed at small businesses progressively increase from year to year (Rahman & Lackey, 2013), with each breach estimated to cost $263,000 (Symantec, 2016). In addition to fending off deliberate cyber-security attacks, small business owners must contend with over 10 million viruses circulating the internet on any given day leaving them vulnerable to unintended exploits (Ethala & Seshadari, 2013). The general business problem is small business owners are not adequately implementing cyber-security strategies, leaving them susceptible to unplanned costs that can bankrupt their business. The specific business problem is that small business owners lack effective strategies to make informed decisions regarding cyber-security investments to protect the businesses from cyber-attacks.

Purpose Statement

The purpose of this qualitative multiple case study was to explore strategies used by small business owners to make informed decisions for cyber-security investments to protect the business from cyber-attacks. One of the biggest issues a company, whether large or small, must face is defending themselves against cyber-attacks (Fielder, Panaousis, Malacaria, Hankin, & Smeraldi, 2016). Cyber-attacks are on the rise, specifically for small businesses (Hutchings, Smith, & James, 2013). However, small business owners often do not implement adequate cyber-security controls.

While all businesses are susceptible to cyber-attacks, small business owners are appropriate for this study because current researchers have suggested they lack the overall resources to identify and mitigate cyber-security threats. The sample for this multiple case study was 10 small business owners from the southeastern United States with successful cyber-security strategies. For this study, successful cyber-security strategies were strategies or measures that have successfully mitigated cyber-security risks resulting in the small business not having a realized cyber-security incident. The participants were from various small businesses that met the United States Small Business Association classification for their type of offerings. The results of this study may impact social change through the improvement of the small business cyber-security climate by providing insight into potential barriers and recommend feasible solutions.

Nature of the Study

I employed a qualitative research methodology for this study. Qualitative research is ideal when exploring areas with unknown variables (Horsewood, 2011) and the method allows for flexibility in data collection through the use of personal interviews and open-ended questions (Yin, 2014). The qualitative methodology is appropriate to study the resources used by small business owners to make informed decisions for security investment and policy decisions. Davies (2015) defined quantitative research as explaining phenomena by collecting numerical data that are analyzed using mathematically based methods (in particular statistics). Quantitative and mixed methods research were not appropriate for this study because there is no established basis of measurement. I asked small business owners open-ended questions that would not produce consistent, measurable results required in a quantitative or mixed methods study.

The selected design for this study was multiple case study. The rationale for the use of a multiple case study was that this case represents a common case (Yin, 2014). According to Yin (2014), a multiple case study allows the researcher to capture conditions related to a particular interest. The multiple case study design is the most appropriate design to use for this study. As affirmed by Yin, case studies are relevant when research questions are explanatory, such as how or why questions, which is the context of this study. Ethnographic, phenomenological, and grounded theory research designs are not appropriate for this study since they focus on culture, lived experiences, and theory.

Research Question

The results of this study may help small business owners understand cyber-security threats and possible strategies to protect their business from these threats. The central research question for this study was:

What strategies do small business owners use to make decisions regarding cyber-security?

Interview Questions

1. What strategies are you using to secure your business from cyber-security attacks?
2. What type of resources did you use to craft your cyber-security strategies?
3. What have you learned through personal experience about securing your business?
4. What training do you have in place for your employees about cyber-security?
5. What role do your employees play in your cyber-security activities?
6. What cyber-security strategies have you implemented but have found are not useful to small businesses?
7. What types of cyber-security strategies would you like to implement but have not?
8. What additional information would you like to share your information security strategies?

Conceptual Framework

The implementation of a successful cyber-security strategy requires an initial and ongoing investment in resources and people (Rahman & Lackey, 2013). The process of implementing and maintaining this potentially complex security strategy can be daunting to those who do not have basic cyber-security knowledge (Wright, 2011). The foundation of this study was that cyber-security strategies are part of the overall business model, or system, and only through acceptance of security technology will a small business be able to implement a successful cyber-security strategy.

To support this study, I selected Bertalanffy's general systems theory as the conceptual framework. According to Bertalanffy, an organization is a complete system involving different parts (Bertalanffy, 1972). These parts include human, social, organizational, and technological subsystems and they must interrelate to achieve the goals of the organization (Baxter & Sommerville, 2010). For this study, the small business was the overarching system. The employees, technology, and strategies comprise the internal components of the system. These parts must cohesively work together to protect the security of the information a small business owner is entrusted to protect.

According to Hayes (2012), small business owners are reluctant to accept cyber-security as a necessity. This reluctance has an overarching effect on the viability of a small business to sustain operations. The interconnection between employees, hardware, and security controls is vital to the success of a small business adequately securing their data (Puhakainen & Siponen, 2010). Specifically, concerning the people making the overarching decisions, the people working on the network, the hardware implemented, and the security controls implemented. The overarching goal is to promote awareness of the interconnection of these components and the relationship to cyber-security to the successful operation of the system.

Operational Definitions

Application: An application is a program that allows users to accomplish tasks utilizing a computer (Raiyn, 2014).

Breach: unauthorized access to sensitive, confidential, or protected data (Sen & Borle, 2015).

Cloud computing: cloud computing allows users to access resources through the internet or network connection remotely (Gupta, Seetharaman, & Raj 2013).

Cyber-security awareness: knowledge of Cyber-security controls, threats, and handling methods (Locasto et al., 2011)

Security Controls: any precaution or countermeasure used to avoid or minimize cyber-security risks (Conner & Conner, 2013)

Assumptions, Limitations, and Delimitations

Assumptions

In research, there are assumptions that are accepted as true, or certain to happen with proof (Bonell, Fletcher, Morton, Lorenc, & Moore, 2013). There were two assumptions related to this study. The first was that participants would answer questions without fear of reprisal or harm to their reputation and business. The second assumption was that the data gathered from interviewed participants would accurately depict what is truly happening. I presented participants with nondisclosure agreements to ease fear of reprisal. In addition, my academic chair verified the validity of the data.

Limitations

Limitations in research are conditions out of the researcher's control (Moustakes, 1994). There were three limitations in this study. The first limitation was that small business owners might inadvertently provide inadequate data due to their limited knowledge of cyber-security. The second limitation was that cyber-security continues to evolve, and that would limit the knowledge of participants. The third limitation was that because this was a multiple case study, the results would be specific to those organizations.

Delimitations

Delimitations are boundaries set by the researcher in a study (Moed, 2010). I limited this study to small business owners located in the southeastern United States. The delimitations of the study were: the sample size, the size of the business, and the location of the business studied. Ten small business owners were sampled to ensure data saturation. The size of the business was limited to small businesses as to control the information received and appropriately direct the findings. I limited the participant population to the southeastern United States for interview accessibility.

Significance of the Study

Contribution to Business Practice

Small businesses are a vital component of the American economy which is evidenced in the federal government outsourcing over $83 billion dollars' worth of work to small businesses in 2013 (SBA, 2013). With this success, small businesses have become targets of cyber-crimes. According to the National Small Business Association's 2013 survey, over 94% of small business owners believe cyber-attacks are a risk to them, and over 44% had fallen victim to a cyber-attack. Small business owners have an urgent need for effective strategies for cyber protection. This study may provide small business owners with a better understanding of strategies required to protect their data from cyber-attacks.

Implications for Social Change

Social responsibility transcends business size and can likely have a positive impact on all society. The intent of this study is to encourage small business owners to protect the data entrusted to them, which will benefit society overall. If small business owners consider an investment in security to maintain or increase financial performance, they may consider security a sustainable business practice. This may, in turn, generate social benefits for the communities in which they operate. These advantages include, but are not limited to, employment opportunities, revenue, and an increased sense of community.

A Review of the Professional and Academic Literature

The purpose of this qualitative multiple case study was to explore strategies used by small business owners to make informed decisions for cyber-security investments to protect the business from cyber-attacks. The literature review included a review of academic journals, commercial print articles, websites, industry white papers, corporate reports, government reports, and presentations. At a minimum, 85% of the academic journals are peer-reviewed and published within five years of this doctoral study. I noted that the pace and rate of change within cyber-security related topics limited sources for peer-reviewed work in not in journal format. To ensure the accuracy and legitimacy of the articles I used the following sources Walden University Library, Google Scholar, ProQuest, SAGE, and EBSCO.

A review of academic and professional literature allowed me to research current cyber-security strategies used by small business owners, the current cyber-security threats faced by small business owners and cyber-security strategies used by large businesses that have the potential to benefit small businesses. Search methods included researching current trends in cyber-security, small business statistics, risk assessments, business plans, strategic plans, and government regulations regarding cyber-security. Accordingly, the specific focus areas will be cyber-security threats, strategies, and cost of cyber-security.

Cyber-Security Threats

Cyber-security threats continue to rise, evolve, and take on a new form. There were 430 million new unique pieces of malware detected in 2015, which is a 36% increase from 2014 (Symantec, 2016). This increase in threats represents a sharp increase from the 10 million malware infections that circulated the Internet in 2010 (Ethala & Seshadari, 2013). With the rising rate of technology adoption by small businesses, this leaves them extremely vulnerable. Malware infections alone have the ability to corrupt, steal, or exploit data. It is vital for small business owners to adopt a cyber-security posture that provides a robust and adaptable layer of protection.

In addition to malware, a new threat has emerged called ransomware. Ransomware is a type of malware that hackers use to lock users out of their computer system (Goldsborough, 2016). Ransomware is a tool utilized by hackers with the intent to extort money from the persons they infect (Everett, 2016; Goldsborough, 2016). The primary targets of ransomware in 2016 were users and hospitals (Goldsborough, 2016). End users are targets because they lack the resources to recover properly from an attack while hospitals are concerned with data integrity and confidentiality (Goldsborough, 2016). Small business owners typically have the same cyber-security controls in place as end users, which make them targets of ransomware (Everett, 2016).

There is an increase in the diversity of ransomware attacks as well as the rationale behind them. In the past, hackers focused on blanket attacks with the attempts of gaining as much money as possible in a short amount of time (Everett, 2016). The new trend is hackers attacking specific businesses with a critical need for their data, such as hospitals, and businesses that cannot recover with any loss of data (Everett, 2016). This targeted approach also lends credibility that small business owners will become prey to hackers who utilize ransomware because they do not have the ability to rebound from a loss of data.

There are many areas of technology that are vulnerable to cyber-security threats. One particular area of interest of researchers is security vulnerabilities associated with consumer electronic systems and the methods used by small business owners to protect that data (Bandar & Christian, 2013; Laszka, Johnson, Schottle, Grossklags, & Bohme 2014). In a survey of small businesses, researchers found that the majority of the small business owners surveyed outsourced their electronic commerce web sites (Laszka et al., 2014). Though outsourced, the IP address and operating system of the server that hosted the site was still visible through a basic Google search. Additionally, the researchers found that the appropriate ports were secure in outsourced sites, and cited the need for more research to ascertain how small businesses that do not outsource their electronic commerce sites handle port security and overall network security (Laszka et al., 2014).

The referenced flaw is an illustration of how small businesses are vulnerable through just publicizing their IP address, something that is quite common.

While the publication of IP addresses is a potential exploit to small business owners so is the use of web technologies. Hutchings, Smith, and Lau (2015) and Lesnykh (2011) theorized there are three main contributing factors that expose vulnerabilities in web technologies. The first is the proliferation of high-end technologies, including Web 2.0. The second is the increasing shift that hackers have taken from targeting information technology infrastructures to targeting data. The third, and largest contributing factor, is insider threat. Consequently, the minimum cost of a single cyber-security breach associated with web technologies was $190,000 in 2011 (Lesnykh, 2011) and has risen to $263,000 in 2015 (Symantec, 2016).

Cyber-terrorism is another form of threat that is becoming a bigger threat to both government and commercial entities (Ahmad & Yunos, 2012; Jarvis, Macdonald, & Nouri, 2014). The threat has materialized at such a rapid pace that researchers have called for a method to establish and test a cyber-terrorism framework (Ahmad & Yunos, 2012; Jarvis, Macdonald, & Nouri, 2014). In one study, researchers found that governments were at greater risk of cyber-attacks followed by computer networks, but businesses with access to government networks had an equal threat (Ahmad & Yunos, 2012). With the continued use of small businesses to perform government work, this is a realistic threat. Without hardening techniques that are capable of adapting to the latest threats, cyber-terrorism will continue to pose a threat to all businesses, regardless of size (Ahmad & Yunos, 2012).

While web technologies are slowly monopolizing commerce so are the use of Smartphone and other mobile devices (Brenner, 2013; Harris & Patten, 2014). With small and medium-sized businesses having a heavy reliance on tablet and Smartphone technology the inability to secure these devices, leave them vulnerable. Small and medium-sized businesses do not have the same monetary capabilities that large-scale enterprises possess to keep pace with these emerging threats (Gordon, Loeb, Lucyshyn, & Zei, 2015; Harris & Patten, 2014). Researchers have called on the academic community to provide additional research and resources to develop cost effective ways to secure the data of small and medium businesses (Gordon et al., 2015; Harris & Patten, 2014).

The use of mobile devices and social media go hand in hand (Chauhan & Panda, 2015). In particular, small businesses are utilizing social media for primary business functions such as recruiting employees or marketing to customers (Chauhan & Panda, 2015). The use of social media applications is a vulnerability or another point of access that business owners need to control (Zhao & Zhao, 2015). Specifically, the protection of the data that are transmitted and stored electronically.

Data storage is a growing concern for large businesses. The way data are shared and stored evolves together with technology. The term Internet of Things (IoT) refers to objects embedded in technology objects to transmit data (Britton, 2016). According to the 2015 State of the Market Report, there will be 5 billion IoT items by 2020. These items can range from microchips, sensors, and actuators. These devices mostly share data through Internet Protocol through software or other communication devices.

Small businesses utilize numerous components that belong to the IoT, specifically smartphones, computers, tablets, and other credit card readers (Ban, Choi, & Kang, 2016). These devices transmit data over the internet through wireless technology such as 4G networks or hardwired Ethernet connections. Data protection is important, regardless of the connection type. Often small business owners adopt this type of technology assuming that it is safe, or that the vendor has ensured the safety of the data. Unfortunately, small business owners must also consider securing data at rest as well as data in transit. While the device the small business owner is using may encrypt data while in transit, they must encrypt any data they store.

Another topic of research is potential exploits within the software of the network infrastructure. Specifically, the platform used to run the servers and network devices on the network. Often networks consist of servers running operating systems such as Microsoft Server or Linux. Microsoft Server has over 45 million lines of code (Britton, 2016) that carry inherent security vulnerabilities. These operating systems are susceptible to malware just as personal computers are. A breach on a server can carry heavier consequences depending on the type of data hosted or connections that server has to other devices.

In 2013, there were over 103,000 open exploits related to Linux, a popular operating system (Avgerinos et al., 2014). In 2015, there were over 100,000 confirmed incidents with 2,164 reported data breaches involving United States companies (Verizon, 2016). With Linux being open source, it is a popular choice for small businesses and companies that are outsourced by small businesses (Avgerinos et al., 2014).

While network attacks will remain a common vulnerability, the need for detecting these exploits is critical. Researchers and industry officials have attempted to control exploits through virus detection software, anomaly detectors, and other scanning apparatus. In one study, researchers created an active exploit program, which they called the automatic exploit generation (AEG), and implemented it in a live environment (Avgerinos et al., 2014). AEG was able to identify buffer flows and detect other anomalies in a network considered secure. Avgerinos et al. (2014) found that the program was effective yet more time and further research should focus on scaling the solution based on network size. Without being able to scale AEG, the program was ineffective in stopping all attacks. The most significant finding from this study was that networks considered secure might have vulnerabilities. These undetected vulnerabilities have the potential to be detrimental to small business owners based on the previously discussed cost of security breaches.

Researchers emphasize threats to infrastructure or hardware while often a cyber-security breach is due to a simple human error (Heidenreich & Gray, 2014). Posey, Roberts, Lowry, and Hightower (2014) performed a qualitative study to measure the perception of security controls and responses to breaches interviewing 22 regular users and 11 security experts. The researchers intended to ascertain whether users know about security controls and feel responses to security breaches are effective. Posey et al. (2014) concluded that both sets of individuals had varying perceptions of both categories. Specifically, the individuals surveyed were not aware of most controls and were unaware of any actions taken. Both groups agreed that the biggest threat was the *insider threat*.

The insider threat is not limited to human error it can also be a deliberate act by malicious employees or compromised employees (Branker, Eveleigh, Holzer, & Sarkani, 2016). Insider threat can take the form of simple theft or ongoing and continues data theft (Branker et al., 2016). Small business owners can be particularly susceptible to insider threat because they often have access to data from larger entities as part of a teaming agreement and lack sophisticated detection methods (Heidenreich & Gray, 2014).

Insider threat has become harder to detect over the years due to the proliferation of technology (Wang, Gupta, & Rao, 2015). In previous years' insider threat was isolated to the employee's specific job role. In any given office environment an employee can intentionally plant malware or other nefarious hacking tools to steal or destroy information. Small business owners may perceive that they do not have information that is of any value to these types of threats, but the threat may lie in the fact that the employee deliberately destroys data.

Another threat that is unknown to most, but prevalent in cyber-threats is shielding (Yener & Cerezci, 2016; Zhang, Zhang, Wang & Lu, 2012) Shielding is the theft of data through radio frequency (Yener & Cerezci, 2016). In multiple studies, researchers have found that the increase in data theft through shielding is rising (Yener & Cerezci, 2016; Zhang et al., 2012). The primary method for data theft through shielding is through intercepting the transmitted data to a liquid crystal display (LCD) (Yener & Cerezci, 2016; Zhang et al., 2012).

Researchers in both industry and academia have focused on the impact of shielding breaches as well as potential methods to decrease the ability to intercept data. In one study Zhang et al. (2012) evaluated information leakage arising from computers and other peripheral devices through shielding focusing on personal impact as well as organizational impact. The variables were the components that make up shielding. The statistical model created was to challenge the existing FCC and MIL 461C models accuracy. The researchers concluded that both the FCC and MIL 461C models were not accurate and that the model created had a greater degree of precision that allows for quantitative measurement of the potential for theft by computer shielding.

Similarly, researchers have sampled commonly used items such as CRT monitors, LCD monitors, laptops, and smartphones for shielding theft to determine which is more susceptible (Yener & Cerezci, 2016; Zhang et al., 2012). The most susceptible item to shielding is an LCD monitor due to the frequency in which it transmits data to the screen (Yener & Cerezci, 2016) with smartphones being almost impenetrable to shielding. These items apply to individuals and all sizes of businesses. The overall intent is a good platform for further research. Specifically, to determine the frequency at which these types of attacks occur and any cost associated with them.

While many researchers focus on threats and vulnerabilities to specific hardware, software, or network platforms, there is a qualitative aspect to cyber-security. In some respects, if a company does not believe they are a target they will not invest in protections. There is an overall lack of cyber-security related literature that goes into depth specifically related to small businesses (Hayes & Bodhani, 2013). The number of academic articles related to cyber-security and small businesses has not grown in proportion to the number of vulnerabilities associated with small businesses (Hayes &

Bodhani, 2013). This disproportional coverage is thought to be contributing factor to small and medium business owners not perceiving themselves as a target, in the same manner, a large company does (Hayes & Bodhani, 2013).

Additionally, Harris and Patten (2014) highlighted the dilemma faced by small and medium businesses in implementing emerging controls for smartphones and tablets. Harris and Patten discussed that small and medium-sized businesses do not have the same monetary capabilities that large-scale enterprises possess to keep pace with these emerging threats. With small and medium-sized businesses having a heavy reliance on tablet and smartphone technology the inability to secure these devices, leave them vulnerable. Harris and Patten provided recommendations for small and medium business owners to implement. Harris and Patten cited a need for additional research to ascertain cost effective ways to secure the data of small and medium businesses.

Cyber-Security Strategies

While cyber-security threats continue to evolve strategies to mitigate and counteract, these attacks must evolve too. Corporations have dedicated teams of cyber-security specialists, the government has specific regulations, and universities have degrees revolving around cyber-security. The average small business owner does not have the skill set required to implement large-scale, proactive network defense techniques, yet needs a strategy (Borett, Carter, & Wespi, 2013). It is important for small business owners to stay abreast of current trends in cyber-security and utilize strategies that make sense to their business (Lanz, 2013).

In addition to cyber-security strategy, there is a necessity for sustainability planning for small and medium businesses (Ates & Bitici, 2011). Specifically, scholars are calling for studies that focus on the need for small and medium businesses to create capability and sustainability plans, keeping mind turbulent times and economic downfalls (Ates & Bitici.2011; Cezar, 2013). According to Ates and Bitici (2011), organizational resilience is achievable with long term planning and proper management planning regardless of business size.

Another claim by researchers is that users with more control over their computer assets are more at ease (Elie-Dit-Cosaque, Pallud, & Kalika, 2011). Essentially, if controls are visibly stringent, it causes anxiety on the part of the end user. Elie-Dit-Cosaque et al., (2011) surveyed students enrolled in a training program and found that an increase in autonomy reduced the anxiety of end users with new technology. The results of this study are important to small business owners as they control their hardware and software most of the time. In understanding what causes anxiety as it relates to security controls, small business owners can properly manage that versus decrease number of controls they have in place.

Sustainability through the process or product innovation lacks in small businesses (Theyel & Hofmann, 2012). Often small business owners lack knowledge of current market trends, or on the innovation of other companies driving an overall sense of insecurity and instability in small businesses as they are unable to sustain without the guidance of industry. An attribute determined by researchers that lend to small business owners thriving and sustaining their business is their ability to communicate with stakeholders about continual improvement and sustainment efforts (Theyel & Hofmann, 2012). Effective communication lends to the credibility of the small business and their ability to manage their work. Developing and testing a cyber-security policy is not only good business, but it is also essential to operating in today’s business environment.

The United States government has initiated reporting mechanisms for industry to share security information with the government to track trends. The government has taken particular interest in small businesses since they are not required to report security incidents through any other legislation (Clinton, 2015). Previous literature and limited government statistics show that small business owners are more susceptible to cyber-security attacks versus large corporations due to their lax controls (Clinton, 2015). Researchers found that companies with strict security controls reported the same amount of breaches as companies without security controls though it could be because companies without strong controls are unaware of breaches (Urciuoli, Mannisto, Hinsta, & Khan, 2013).

Companies can utilize risk management techniques to reduce cyber-security threats. Risk management is a technique that would particularly benefit small business owners due to the low cost involved with learning how to perform risk assessments. Researchers reviewed two recent surveys performed that assessed companies risk assessment procedures and found that 68% of the respondents indicated that their CEO is placing greater emphasis on risk management (Barles, Cote, & Williams, 2012). Also, only 35% of the respondents indicated that they had a formally trained executive or business line manager capable of properly assessing risk. Furthermore, the researchers found that 55% of the respondents indicated that no one in senior management was responsible for risk management or mitigation (Barles et al., 2012).

Another area of academic research is the lack of anti-fraud controls instituted by small businesses, leaving them vulnerable to security breaches (Tysiac, 2012). In an extensive literature review, Tysiac (2012) found that only 56% of small businesses underwent external audits of their financial documents, as compared to 96% of large firms. ACFE also found that only 18.5% of small business employees received training in fraud detection and prevention. The indication of the lapses in security controls had negative repercussions on unidentified fraud experienced by small businesses. Specifically, small businesses found one of three fraud violations by accident versus through vigilant activities or countermeasures.

The issue of expanding Sarbanes-Oxley to small businesses is another area of research that is prevalent in academia (Dey & Sullivan, 2012). The implementation of security measures required to be compliant with Sarbanes-Oxley may be too expensive for small businesses, and the cost would outweigh the benefits (Dey & Sullivan, 2012). The adaptation of internal audit procedures similar to those required in Sarbanes-Oxley may be a viable solution for protecting small businesses from cyber-security attacks (Dey & Sullivan, 2012).

The use of managed service providers, or MSSP's, is another viable alternative for small business owners (Hui, Hui, & Yue, 2012). The use of MSSP's is on the rise, especially in the United States. Small business owners utilize MSSP's to perform penetration testing, security assessments, and security planning. While MSSP's have a distinct advantage over not performing these tasks, there is an inherent risk associated with system interdependency. System inter-dependency, according to Hui et al. (2012), is the unintentional spread of viruses or other vulnerabilities using the same MSSP. Specifically, the MSSP may handle a security incident for one client and unintentionally passes the vulnerability to other, either through the inability to detect the vulnerability in time or through improper controls. Having viable alternatives is especially important to small business owners as it gives them an alternative method of performing cyber-security related work.

While hackers are a known threat to any business, they can also prove to be beneficial in some cases. The study of utilizing ethical hackers is popular among researchers and industry alike (Conrad, 2012; Steinmetz & Gerber, 2016). Specifically, Conrad (2012) recommends that small and medium-sized businesses utilize ethical hackers to perform penetration testing on their networks. The belief is that small and medium-sized businesses do not perform penetration testing or network security outside normal virus protection. The use of ethical hackers could greatly increase the security posture of small networks without incurring the cost of hiring full-time security personnel.

The utilization of existing solutions can be an efficient alternative for small business owners. In particular, the use of existing frameworks that provide a solid foundation with a sense of flexibility can increase the likelihood of establishing a successful cyber-security strategy (Hoy & Foley, 2015). One such existing solution is cyber-security frameworks such as ISO 27001 or COBIT. These standards are established with the input of industry and by building off of known best practices (Hoy & Foley, 2015).

Standards like ISO 27001 and COBIT provide users with a framework to follow based on industry best practices but do not dictate specific requirements (Hoy & Foley, 2015). For example, the ISO 27001 requires users have a password policy but does not dictate the content of the policy or the requirements. Also, small business owners who adopt any ISO standard can become certified. The certification process includes having a licensed external auditor from an accredited company evaluate the company’s adherence to the standard. The cost of an external appraisal is significantly less than hiring a consultant to evaluate processes and can be an inexpensive way to get an outsiders perspective (Hoy & Foley, 2015).

The ISO 27001 standard is flexible in that can be utilized for any business that employs information technology (Hoy & Foley, 2015). Small businesses in the medical field that require extra controls to protect protected health information would benefit from the use of the ISO 27001 standard. Compliance with ISO 27001 is ideal for medical organizations as it would assist in addressing network, data, physical, and human security controls (Liao & Chueh, 2012). A survey of medical professionals that currently utilize ISO 27001 as a security management system found that risk management was more thorough, employees were better trained, and incidents decreased (Liao & Chueh, 2012). The robustness and interaction employees have with the security management system is a benefit to small businesses that do not employ a large cyber-security team (Hoy & Foley, 2015; Liao & Chueh, 2012).

Another area of research is the use of COBIT in conjunction with the ISO 27001 standard (Razieh & Nasser, 2012; Sheikhpour & Modiri, 2012). In one study, researchers compared the ISO 27001 standard to the COBIT standard to identify similarities (Razieh & Nasser, 2012; Sheikhpour & Modiri, 2012). The researchers found that ISO 27001 focuses on integrity, confidentiality, and availability of resources whereas COBIT is more focused on network security (Razieh & Nasser, 2012; Sheikhpour & Modiri, 2012). COBIT focuses on these areas; it does not provide a strong enough framework to implement COBIT effectively.

Other researchers focus specifically on utilizing COBIT 5 as a security framework for small businesses (Thomas, 2013). In one case study, Thomas (2013) monitored the implementation of COBIT 5 in a small certified public accounting firm. The firm consisted of 140 employees and 21 shareholders. The firm had six locations including employees who worked remotely or at client sites. The details included glitches, cost, setbacks, and usability and found that COBIT 5 is an efficient way to organize and integrate IT functions with the overall organization (Thompson, 2013). The CPA firm that utilized COBIT was able to focus on mitigating risks more effectively versus trying to implement strategies.

While compliance is often studied, other areas of research include the necessity and benefits ISO 27001 certification (Cohen, 2011). This area of the investigation came about due to the requirement for compliance with the standard is required for all companies bidding on work in the United Kingdom. To show compliance United Kingdom companies must complete a lengthy survey that maps compliance to the ISO 27001 standard. On the contrary, companies that were ISO 27001 certified were often given a waiver from filling out the survey due to the complexity of ISO 27001 and the external audit procedure (Cohen, 2011). Also, Cohen found that a company could request an extension if they were out of compliance if they were able to show a project plan showing they were working towards complying with or obtaining an ISO 27001 certification. Cohen believed that companies could benefit from following the ISO 27001 standard, and if possible, obtaining the certification. The overall cost is minimal; so small businesses can afford to get the certification.

The return on investment and overall benefit for obtaining ISO 27001 are other relevant areas of research. The two leading adopters of ISO 27001, by way of external audit, are Japan and the United Kingdom (Everett, 2011). The majority of industries in the United States that did obtain the ISO 27001 certification were defense contractors, telecommunications, energy companies, and financial companies (Everett, 2011). Retailers small businesses were not embracing the standard though they could utilize it for a framework that is proven and stable. Also, ISO 27001 is ideal for small companies and retailers because it stimulates employee training and accountability (Everett, 2011).

Similarly, Kanynak and Karagöz (2014) explored the slow rate of adoption for the ISO 27001 standard versus ISO 9001 and ISO 14001. ISO 9001 focuses on quality management, and ISO 14001 focuses on environmental protection. The research intended to find cost-effective ways for companies, specifically small businesses, to adopt the ISO 27001 standard. One trigger for this research was the recent adoption of ISO 27001 by governments. In particular, the Japanese government mandates ISO 27001 certifications for companies that handled sensitive data which is similar to the United Kingdom requirements (Kanynak & Karagöz, 2014).

Another important area of cyber-security is risk management. In one study, researchers explored why business managers the necessity, efficiency, and investment worth of risk management while making risk management accessible to those without IT knowledge (Baily, Migilio, & Richter, 2014). They developed a user-friendly software solution that they implemented in two qualitative studies. They concluded that the risk management software, through its intuitiveness, allowed companies to identify more risks, more efficiently, and with improved accuracy (Baily et al., 2014).

In addition to identifying potential risks and vulnerabilities, companies must deploy appropriate countermeasures to mitigate risks (Schuessler, 2013) As with risk identification, companies that do not employ security experts should utilize industry reports and trending analysis. Industry, academia, and government entities publish reports that detail the exact results ranked the most common exploits and vulnerabilities as well as the most efficient controls at the time of the report.

There is an increased adoption of cloud computing among small and medium business owners (Beckers, 2013). Researchers believe five factors influence the adoption of cloud computing (Gupta & Seetharaman, 2013). The factors are ease of use, security and privacy, cost reduction, collaboration, and reliability. The researchers utilized a qualitative structural equation to test 14 hypotheses. The researchers administered a survey to small business owners who utilized cloud computing and found the strongest relationship exists between cost reduction and cost savings (Gupta & Seetharaman, 2013).

Another emerging trend in technology is the use of cloud computing. Cloud computing is growing in popularity among individuals, businesses, and government entities (Georgescu & Suicimezov, 2012). Cloud computing allows users to store data in a remote location that is maintained by another group. While cloud computing can enhance productivity, and protect data from loss Georgescu and Suicimezov (2012) found that users who adopt cloud storage methods and completely disregard risk management and mitigation activities associated with local onsite storage. Georgescu and Suicimezov contend that cloud computing requires a special risk assessment and additional security precautions apply to the user. Georgescu and Suicimezov recommended further studies to apply a framework that accounts for confidentiality, availability, and integrity.

While there are many resources available to small and medium businesses alike, it is unknown what fosters adoption of these standards. In one study researchers and explored user acceptance techniques as they relate to cyber-security activities (Wang, 2014). Wang and Wang (2014) created a model for user acceptance predictability based on current technology, utility, cognitive cost, and self-efficacy. Wang and Wang verified the data as being efficient and offer additional advice for Chinese firms to utilize when implementing cyber-security activities. Further research can be done to validate if these techniques will benefit all small businesses or a subset.

In addition to compliance and adoption techniques, researchers also focus on the need to create a culture that is rich in cyber-security awareness to enhance the overall safety of the network (Alhogail & Mirza, 2014). One belief is that adopting a change management process that includes cyber-security considerations for all changes to the network (Alhogail & Mirza, 2014). Incorporating cyber-security into change management decreases the chances of making a change that can create vulnerability on the network. Ultimately, all businesses should adopt simple change management processes regardless of the size of the business.

While technology evolves constantly, there is a trend in innovation and adoption of mobile technology in public health (Currie and Seddon, 2014). As of 2014, more public health institutions were creating mobile medical technology products to meet consumer demand (Currie & Seddon, 2014). The contention is that while social innovation is growing the creation of models and testing against these models have not kept pace. According to researchers, most innovation is due to comparative analysis in varying regions (Currie & Seddon, 2014). Research shows that consumers' desire mobile health technology and by 2016, there could be over three billion active users of internet technology. This progression and continued adoption of technology should be an indicator to health care institutions to adopt mobile technology.

An additional area of study is the influence of emotions on cyber-security behavior (Gulenko, 2014). In one case study, Gulenko (2014) attempted to correlate motivation techniques for individuals and adherence to cyber-security policies. The researchers compared the findings to the technology acceptance model, innovation diffusion theory, and the social cognitive theory and found that positive words used in information systems security were effective in establishing secure habits (Gulenko, 2014). Subsequently, negative words are effective when breaking negative habits (Gulenko, 2014).

Furthermore, Lebek et al., (2014) performed a study that comprised of a literature review of 113 publications aimed to identify applied cyber-security related theories within the last decade. The authors found that only 4 of 54 theories were being used by researchers; the theory of planned behavior, general deterrence theory, protection motivation theory, and the technology acceptance model. The analysis also showed that there are specific factors that have proven to be a more significant influence on security behavior.

Cost of Cyber-Security Breaches

Cyber-security has become a consideration that managers must consider when planning their budget (Gupta, 2011). In particular, managers must know how to fund according to their threat model. In one case study, Gupta (2011) comprised funding models through the perspective of a small business and an attacker. The strategic portion of the model allows companies to identify funds needed to cover technology, security, continuity activities, and infrastructure. The other part of the model is a risk management module and allows companies to allocate money to items specific to protecting their risks. The model was efficient and is adaptable for small and medium businesses (Gupta, 2011).

The consequences of a data breach can be devastating to small businesses. In one case study, researchers looked at historical stock market data and compared firms that reported a violation to those who did not (Gordon, Loeb, & Lei, 2011). The researchers utilized the basic one-factor CAPM model and FAMA-French three-factor model to calculate the stock return 121 days before and three days after a security breach and concluded that the stock remained unchanged after a security breach (Gordon et al., 2011). The lack of financial ramifications is often perceived as a factor for small businesses not adopting security controls.

Building upon previous literature Watts (2011), discussed the recent decision by the SEC to continue and allow companies who float under 75 million a year to opt out of Sarbanes-Oxley. While there had been calls from scholars, academics, politicians, and large corporations alike for equal treatment, the SEC could not find the justification in the cost for businesses that did not gross profit over 75 million. The results of this study can be helpful to small business owners because, years later, the contention is that still, those small businesses need oversight in financial and other reporting.

While small businesses do not require Sarbanes-Oxley, it can be effective in establishing a cyber-security framework (Kinney & Shepardson, 2011). Between 2003-2008, small businesses undergoing 404 (b) audits experienced a statistically significant increase in weaknesses discovered during these audits (Kinney & Shepardson). Also, it researchers found that the small firms did not correct the audit findings. The rationale behind this was the increase in cost for not only audits, which doubled during that period, but the remediation costs.

There has been a growing need for a tool that can anticipate the possibility of the company failing based on several attributes (Borrajo, Baruque, Corchado, Bajo, & Corchado, 2011). In one study, researchers created a model that incorporates inputs regarding purchasing, cash management, sales, asset management, human resources, and information technology (Borrajo et al., 2011). The researchers grouped the processes into functional areas with information technology including cyber-security activities and tested the prototype on small businesses. The results were both useful to the researchers collecting data and the business owners that participated in the study. The business owners were able to see potential pitfalls in their investments, and how modifications to each can change the others, potentially for the good or bad.

Data shows that half of all new small businesses survive after four years yet there were a sufficient number of studies to ascertain why this phenomenon occurs, but the data collection is done mostly through businesses that did survive which skews the data (Cader & Leatherman, 2011). To confirm this belief, the researchers conducted a study utilizing the Cox Accelerated Failure Time Model and found that the data collection is not truly adequate thereby giving small business owners a false sense of security.

Samujh (2011) explored the issues involving small business sustainability. Smaujh (2011) performed literature reviewed followed by a qualitative grounded theory study to ascertain the reasons why small businesses often fail. Smaujh (2011) was able to gather 91 usable questionnaires. Smaujh (2011) concluded that small business owners lacked formal business training, were unable to maintain their business without working over 60 hours a week and had little documented in the areas of business planning and sustainability. Smaujh (2011) concluded that small business owners lacked sufficient resources to assist them with basic business planning, including financial backing to implement sustainability plans.

Researchers contend that there is a connection between market competitiveness and small business strategy (Salazar, Soto, & Mosqueda, 2013). Specifically, the researchers believe there is a relationship between funding decisions and market longevity and subsequently found that small business owners in their region lack competitiveness due to intensive strategies and lack of long-term investment plans. Also, the researchers found that companies that managed their short-term assets and liabilities are more competitive and survive longer in the market (Salazar et al., 2013).

In addition to sustainability, researchers also focus on innovation and whether small businesses can keep up with rapid advances in technology (Pirta & Strazdina, 2012;

Theyel & Hofman, 2012). The researchers were able to ascertain that recent events, including media coverage, community advocacy groups, and customers influenced more small companies to implement sustainability plans and activities which are a vital area of research for the future sustainability efforts of small businesses.

There is an overarching belief in industry and academia that information technology controls lower risk and reduce overall costs through mitigation of security risks (Pirta & Strazdina, 2012). In one study, researchers found through a comparison of 61 companies and their security controls that companies that implemented controls had a higher success rate in passing financial audits (Pirta & Strazdina, 2012). The researchers also found that these companies also had less risk and fewer incidents involving breaches (Pirta & Strazdina, 2012).

Additionally, Hayes (2012) considered a customized model for technology acceptance. Hayes posits that a visual diagram explaining the new technology and the usefulness to the adopter is a better indicator of acceptance than previous models. According to Hayes, this would be useful for small business owners who have a low adoption rate of technology. Hayes created a template based on the diffusion of innovation theory and the technology acceptance model. Hayes interviewed small business owners to gauge their response to the model. Hayes found that the small business owners were more receptive of the model due to the visual representation of the technology, cost, and benefits.

Furthermore, Rahman and Lackey (2013) explored the common security flaws present in small business e-commerce sites. Specifically, that a small business owner is less likely to follow established security standards and guidelines created to guide them to secure their sites. Rahman and Lackey (2013) discussed common vulnerabilities found in e-commerce sites and the prevention of these attacks. The researchers found that hackers are targeting small business owners more frequently due to their inability or unwillingness to spend money to protect their assets and concluded that small business owners should hire outside firms or individuals regardless of the cost to stay competitive and secure their data.

Little research exists on how to adapt to future changes in technology and how that can affect small business research and development firms. Teirlinck and Spithoven (2013) explored the role of small business research and development firms and their reliance on the key technology. Teirlinck and Spithoven performed a mixed methods study and found that internal innovations directly relate to the external environment. Likewise, Teirlinck and Spithoven found that firms that had strategic plans were more successful in market positioning and longevity.

In addition to security controls, small business owners should implement Emergency Response & Business Continuity plans (Nicoll & Owens, 2013). The impact on a small business that does not have adequate plans in place is catastrophic and can affect the small businesses ability to stay in business compared to a large business. While the previous researchers suggest small business owners had previously been reluctant to spend the money on the development and sustainment of these plans, the view appears to be changing which is pertinent because it assesses the need for small business owners to implement appropriate emergency response and business continuity plans. Also, Nicoll and Owens (2013) also cite previous literature pointing to the need for small businesses to get more in tune with large businesses when it comes to cyber-security controls and plans.

Stephen and Apilado (2013) built upon previous research that suggests that companies are better off because of the Sarbanes-Oxley Act due to the stricter security monitoring guidelines; this was to include smaller businesses that were not required to participate in Sarbanes-Oxley. Stephen and Apilado found that large firms benefit from the analyst security oversight and public reporting mechanisms, which has increased the values of companies over time. Stephen and Apilado found that smaller companies benefit from the overall lack of oversight and reporting requirements.

There are substantial benefits in following an industry security standard since it is a proven framework that is accepted and adopted by many in the same industry. Many companies that follow a cyber-security framework were able to plan better for continuity activities and mitigate risks (Ramanauskaitė, Olifer, & Goranin, 2013). Retailers and small businesses are not embracing the standard though they needed it most as they do not employ full-time security analysts (Ramanauskaitė et al., 2013). Ramanauskaitė et al., (2013) found that following a security standard was ideal for small companies and retailers because it pushed employee training, and was more cost effective than hiring an outside consultant.

Small businesses should also consider the cost of protecting new technology assets when investing in them (Raiyn, 2014). New technology is often susceptible to the attacks such as denial of service, access attacks, cyber war, and passive attacks until the vendor can release patches (Raiyn, 2014). The cost of actively monitoring a network is something that small businesses cannot afford, though they actively handle electronic commerce, personally identifiable information, and government information (Raiyn, 2014).

Eastman, Iyer, Liao-Troth, Williams, and Griffin (2014) explored the relationship between millennials involvement and purchase behaviors as it relates to mobile technology. According to the Eastman et al., research shows a trend indicating that the millennial generation has different values, and buying behaviors compared to previous generations. Also, Millennials have a higher spending power. The millennial generation also has become highly dependent on mobile technology and social networking. To study the relationship between millennials involvement and purchase behaviors as it relates to mobile technology Eastman et al. used the social comparison theory. Eastman et al. found that the level of innovations affects the usage among the millennial consumers. Additionally, users of technology are millennials and may be willing to invest more money in a product for the sake of security (Eastman et al., 2014).

Akhtar, Azeem, and Mir (2014) studied the impact of utilizing information technology, specifically the internet, within small and medium businesses. Specifically, Akhtar et al., contend that small and medium businesses are shying away from utilizing internet technology for several reasons. The first proposed reason cost. Small and medium businesses do not have the funds to finance a significant internet presence as large businesses do. Second, small and medium businesses do not have the capabilities to sustain internet technology related investments. Small and medium businesses could, and should, utilize outsourced technology, like the cloud, to improve their business offerings possibly allowing small and medium businesses to have a similar presence as large businesses and expand internationally.

Researchers often utilize systems theory to explore safety and security based decisions (Young & Leveson, 2014). According to Young and Leveson (2014), safety and security are requirements for every business and should be part of every system. There has been significant focus on security in scholarly study, but not to the point that shows individual firms or corporations how to embed these activities into their overall system (Young & Leveson, 2014). Without considering these functions, where applicable, the entire subsystem is in jeopardy due to inconsistency and lack of planning.

In conclusion, the literature supports the intent of this study and problem statement. While technology continues to evolve, cyber -security is a relatively new field that has a limited number of extensive studies and models. Cyber-security continues to present itself as a viable field of study due to the risk it presents to businesses of all sizes. It is clear that small business owners face the same, if not more, cyber-security threats as large businesses. It is also clear that small business owners do not have access to viable resources to make informed decisions regarding cyber-security techniques within their business. The impact and cost associated with a single cyber-security breach can be catastrophic to small businesses and warrants further research.

Transition

Section 1 included information supporting the research problem. Additionally, a foundation and background presented supporting the phenomenon that small business owners lack adequate resources to address cyber-security. The problem statement addressed both the general and specific business problem while the purpose statement included justification for the selected research method, design, and participant pool. An extensive literature review supported the rationalization of the research problem. The overarching themes of the literature review were; cyber-threats, cyber-security strategies, and the cost of security breaches. Section 2 of this study will include a framework of the research components, further detail on the overall intent of the study, participant enlistment, data collection, and analysis. Section 3 of this study will contain a formal presentation of the findings and proposals for the application of the information collected.

Section 2: The Project

Purpose Statement

The purpose of this qualitative multiple case study was to explore strategies used by small business owners to make informed decisions for cyber-security investments to protect the business from cyber-attacks. One of the biggest issues a company, whether large or small, must face is defending themselves against cyber-attacks (Fielder, Panaousis, Malacaria, Hankin, & Smeraldi, 2016). Cyber-attacks are on the rise, specifically for small businesses (Hutchings, Smith, & James, 2013). However, small business owners often do not implement adequate cyber-security controls.

While all businesses are susceptible to cyber-attacks, small business owners are appropriate for this study because current data suggests they lack the overall resources to identify and mitigate cyber-security threats. The sample for this study was ten small business owners from the Southeastern United States with successful cyber-security strategies. For this study, successful cyber-security strategies were strategies or measures that have successfully mitigated cyber-security risks resulting in the small business not having a realized cyber-security incident. The participants were from various small businesses that met the United States Small Business Association classification for their type of offerings. The results of this study may impact social change through the improvement of the small business cyber-security climate by providing insight into potential barriers and recommend feasible solutions.

Role of the Researcher

My role as a qualitative researcher involved selecting participants and conducting interviews to collect data relating to the study problem. Qualitative research is unique in the fact that the researcher serves as the instrument for creation, administration, and validation of the interview questions (Pezalla, Pettigrew, & Miller-Day, 2012). A qualified qualitative researcher must have sufficient knowledge in the field to understand why the study topic is relevant and to interpret the information as it presents and adjusts data collection activities as needed (Baškarada, 2015; Yin, 2009).

Technology has enveloped the business world making it almost impossible to have a business that does not use technology driving the need for security solutions for all business sizes (Kivimaa, 2013). I have over 15 years of experience in the information technology field, with more than six years focusing on cyber-security, primarily through process implementation and process improvement. I have implemented ISO 27001 in several settings and have done a compliance crosswalk between the ISO 27001 standard and various NIST documents. I believe that companies of all sizes, especially small businesses, require a vigilant, proactive approach to cyber-security.

I interviewed small business owners to explore the reasoning they utilized when selecting the security controls to implement. I served as the interviewer of the 10 selected study participants. I had direct interaction with the selected study participants during the interview process, via concentrated, semi structured interviews. I asked the identified research questions in hopes of the participants sharing their lived experiences allowing me to build a theoretical construct based on qualitative evidence (Eisenhardt, 2007).

To ensure the data collected were accurate and unbiased, I only selected participants that I had not formed personal relationships outside the working environment. During the interviews, I encouraged the participants to speak openly, and completely, to ensure their point of view is of the participants and not my own. Additionally, I remained neutral so that I did not influence my participant’s answers (Baškarada, 2015).

As a researcher, it was my duty to perform this study with the highest ethical standards in mind. I adhered to basic ethical principles established in the Belmont Report. These basic principles ensured respect, beneficence, and justice to all my participants (Belmont Report, 1979). Utilizing the Belmont Report, I ensured my participants had informed consent, will benefit from my research and suffered no harm resulting from their participation.

In all research, it is of particular importance to minimize bias. In qualitative research, there are several ways a researcher can reduce bias. Particularly, researchers can interview hierarchical levels of informants, utilize interview methods that are not face-to-face, or simply interview more than one informant (Eisenhardt & Graebner, 2007). As an experienced subject matter expert in my field, I set aside bias and the urge to prompt individuals for more information. I did this by asking open-ended and specific questions and asking for more detail when needed rather than filling in what I believe the answer is. When I completed transcribing the results of the interview, I asked the participants to review the transcription to be sure that I gathered their sentiment exactly.

When performing interviews, it was important to establish and adhere to an interview protocol. An interview protocol allows an interviewer to gather consistent areas of information (Hill, Knox, Thompson, Hess, & Ladany, 2005). To establish an effective protocol, I have developed my questions based on current literature and trends in the field (Hill et al., 2005).

Participants

The sample for this study was 10 small business owners from businesses in the Southeastern United States with successful cyber-security strategies. For this study, successful cyber-security strategies were those that have successfully mitigated cyber-security risks resulting in the small business not having a breach. A breach was an incident of unauthorized access to data, networks, or applications by bypassing security devices (Gao, Zhong, & Mei, 2015). Physical security was not a consideration for this study. The participant’s businesses also met the criteria established by the U.S. Small Business Administration (SBA) specific to their North American Industry Classification System (NAICS) code dated 2012 or later.

I selected participants from companies with which I currently worked and from government information technology contractors in companies within my industry. Selecting participants from this subset will assist me in establishing rapport (Yin, 2014) which was ideal since nine out of ten unsolicited requests are often ignored (Pan & Tan, 2011). I believe this was a distinguisher for the study because it promotes inclusion of an often-overlooked subgroup, small businesses.

Once I had approval from the Walden Internal Review Board (IRB), I contacted potential participants in person, over the phone, or through written correspondence. I performed in-person interviews when possible to maximize the time spent with each participant. When a business owner indicated a willingness to participate in the study, I asked them to complete and sign an informed consent form. By Walden University's ethical guidelines, all consent forms will are stored for at least five years, and then shredded.

Research Method and Design

Qualitative research is ideal for understanding multifaceted interactions between individuals and their environment (Anderson, Leahy, DelValle, Sherman, & Tansey, 2014). Utilizing a multiple case study approach allowed me to target small businesses and their specific interactions with cyber-security controls. Semi structured interviews allowed me to gather data in the form of the participant's experiences. Through analysis, gained a deeper understanding and insight into prevailing themes that emerged.

A multiple case study approach was an appropriate choice for this study because, by definition, a case study is exploratory and descriptive (Anderson et al., 2014). Additionally, qualitative research allows a researcher to look at the interaction between an individual and their environment (Anderson, 2013). Utilizing a case study, I was able to explore the rationale used by small business owners when implementing cyber-security policies.

Research Method

Qualitative research in cyber-security research has gained significant acceptance among scholars over the years due to the robust and exploratory nature of the research methods associated with it (Stirling, 2001). Qualitative research allows researchers to gain a holistic view of a particular area of interest in areas that do not have enough data for quantitative studies (Sinkovics & Alfodi, 2012). Cyber-security data is hard to quantify making a quantitative research method impractical (Choucri, Madnick, & Ferwerda, 2014) In this instance you cannot quantify the rationale for not implementing controls that only measure the effects of not doing so. It was not my intent to quantify the decision rather understand why small business owners do not implement security controls. To gain the best insight into the cyber-security policy decisions made by small business owners an exploratory method such as qualitative was ideal.

Research Design

During the design phase of this study, I considered several research designs. Specifically, I considered a phenomenological design because it would have allowed me to interview participants and to observe them gather information (Chwalisz, Shah, & Hand, 2008). However, phenomenological requires at least 20 participants, which would have proved difficult to find. Additionally, I considered a narrative design because it allows participants to tell their story in regards to a particular topic (Ketelle, 2010). After careful consideration, I decided against the narrative design because the participants may not have a story, and the data would be more accurate if, as a researcher, I was able to ask pointed questions. I did not consider ethnography because it focuses specifically on shared and learned behaviors (Creswell, 2007). I ultimately selected a multiple case study design because it offered an exploratory and explanatory approach (Anderson, 2014).

Population and Sampling

The criteria for selecting the small business owners that will participate in this study will include: participant's businesses met the criteria established by the U.S. SBA specific to their North American Industry, classification system (NAICS) code dated 2012 or later, had not had a cyber-security breach in the last 12 months, the main office resided within the Southeastern United States, and had been in business at least one year. Engaging this specific criterion allowed for a look into some of the most frequently used small businesses that should have a strong cyber-security program. Additionally, the owners of these types of businesses had more exposure to cyber-security policies and regulations that would assist in obtaining accurate results.

I used purposeful sampling to select the participants of this study. The study included a purposeful selection of ten small business owners or decision makers. Purposeful sampling allows a researcher to access strategic informants in the field who can help rapidly identify information-rich cases (Suri, 2011). This purposeful sampling intended to reach data saturation.

Data saturation is when no new data or information is needed, no new coding or themes, and the study is replicable (Guest, Brunce, & Johnson, 2006; Walker, 2012). Failure to ensure data saturation can have an adverse effect on the overall study (Fusch & Ness, 2015). The most significant result to achieve in data saturation is the collection of rich data versus a large quantity of data (Fush & Ness, 2015). To ensure proper saturation, I established a robust set of inclusion criteria. The more inclusive a researcher is, the more homogeneous the study becomes (Robison, 2014). Utilizing this criterion ensured a successful qualitative study in that it other researchers can replicate the study, I have obtained all the information available, and I can no longer code the data (Fusch & Ness, 2015; Guest et al., 2006; Walker, 2012).

Ethical Research

It was important for me as a researcher to conduct this study with the utmost ethical conduct. The very foundation of ethical research is the informed consent process (Hardicre, 2014). Informed consent is the process in which a participant must affirm in writing that they understood all aspects of the study and agreed to participate (Hardicre, 2014). Participants signed the Letter of Research Scope and Introduction.

I used the Letter of Research Scope and Introduction to provide participants the details of the study, the requirements for participation, and acknowledge that they understand that they have the right to withdraw at any time. It was important for participants to understand the study was voluntary and there were no repercussions for their withdrawal (Hardicre, 2014). To withdraw the participants had the choice to verbally tell me that they wished to withdraw or notify me in writing. I utilized all available resources to ensure the safety of the data I collected. To comply with Walden University standards, I secured all interview results for five years at which time I will destroy them. Additionally, I informed the participants that there was no monetary compensation for the study, which was important so that the participants did not participate solely for money (Hardicre, 2014).

Data Collection Instruments

In this qualitative study, I was the primary data collection instrument (Yin, 2012). This qualitative multiple case study involved semi structured face-to-face interviews with 10 small business owners. The interviews consisted of me asking the predetermined questions in the Interview Protocol. As in all qualitative studies, I interpreted the data (Xu & Storr, 2012).

Qualitative methods do not often entail utilizing strenuous procedures; rather they rely on decision making of the researcher in the field (Collins & Cooper, 2014). Utilizing a semi structured interview technique allowed me to adapt the questions asked based on the answers given (Postholm & Skrøvset, 2013). The ability to adapt is especially effective when the researcher has experience in the field of study (Xu & Storr, 2012). Semi structured techniques are effective in minimizing bias because the researcher does not need to imply what the participant said; rather a researcher can ask clarifying questions to obtain a definite answer (Xu & Storr, 2012).

I utilized a digital recorder to record interviews with the permission of each participant. Additionally, I took detailed notes of all the participant’s answers. Once the interviews were complete, I transcribed the sessions to ensure I captured the full context of what the participant stated. To ensure validity and reduce bias I had the participants review the data analysis regarding their answers.

Once the interviews were complete, I looked for emerging trends in the data (Rowley, Jones, Hanna, & Vasileiou, 2012). Additionally, I looked for potential subthemes. Once that was complete, I started to categorize data from the interviews into these themes. I elaborated on the themes and theories developed from the data analysis in Section 3 of this study showed the alignment with the context of this study (Rowley et al., 2012).

Data Collection Technique

My two primary sources of data collection were face-to-face interviews and a review data from current academic and commercial sources. Before conducting the interviews, the participants signed a consent form. I verbally explained the consent form to the interview participants. In particular, I wanted them to understand that I would be recording the interviews, concealing their identity, the study was voluntary, that they could withdraw from the study at any time without repercussions, and there was no compensation for participating in this study.

I utilized semi structured face-to-face interviews for this study. The interviews took place in a neutral location selected by the participant and lasted between 30-60 minutes. Employing semi structured interview questions allows the researcher to garner a deeper understanding of the topic through conversation style interviews (Rowley, 2012). Also, semi structured interview questions allow for more elaboration that online surveys (Vaismoradi, Turunen, & Bondas, 2013).

Qualitative research allows researchers to gain a holistic view of a particular area of interest in areas that do not have enough data for quantitative studies (Sinkovics & Alfodi, 2012). Interviewing is the primary method of performing qualitative research (Ibrahim & Edgley, 2015). Member checking is a vital component of qualitative research (Carlson, 2010). Member checking is the process in which the researcher has the participants review the transcription data after the fact to ensure accuracy. During the interviews, I utilized a digital recording device, paper, and pen. I transcribed the recordings after the interviews and transferred them to digital media for review by the participants.

Data Organization Technique

I followed a strict interview protocol that allowed me to conduct uniform, consistent interviews (Jacob & Furgerson, 2012). I closely followed the outlined interview protocol I established. I opened all interviews with a brief introduction of myself and my experience and concluded by thanking the participants for their participation in the study. To organize my data and to take notes, I utilized a research journal in addition to a digital tape recorder. I secured all data collection instruments for no less than five years at which time I will destroy it.

I ensured that the data I collect accurately depicts the participant’s views. To ensure the validity and accuracy of my transcribed data, I compared it to the audio recordings (Collins, Onwuegbuzie, Johnson, & Frels, 2013). Also, I analyzed the data for patterns and similarities by categorization data from the interviews and analyzing the data for themes (Baškarada, 2014). I utilized Microsoft Excel to type the data and categorize and record themes from my notes and recordings.

Data Analysis

Once I was content with the accuracy of the data, I entered it into MAXQDA. MAXQDA is a qualitative data analysis software that researchers utilize to collect, organize, and analyze data from interviews, documentation reviews, and field notes. I utilized MAXQDA to formulate themes and codes. I compared several data analytic software applications such as QSR, NVivo, and ATLAS and selected MAXQDA for ease of use. Additionally, I had access to users who have experience in MAXQDA.

Data triangulation also allows a researcher to form a better understanding of the phenomenon (Carter, Bryant-Lukosius, & DiCenso, 2014). In this qualitative multiple case study, I used methodological data triangulation to triangulate data from interviews, academic sources, and commercial sources. The methodological data triangulation allows a researcher to utilize several qualitative methods to corroborate findings (Bekhet & Zauszniewski, 2012). Methodological data triangulation consists of the researcher using multiple forms of data to provide a better understanding of the topic (Bekhet & Zauszniewski, 2012; Denzin, 1978).

In this study, I utilized interviews and review data from current academic and commercial sources as my sources for data triangulation. The data I collected assisted in answering my research question of how small-business owners make informed decisions on cyber-security investments to protect the business from cyber-attacks? I triangulated the analysis and trends I discovered through data analysis against academic and industry resources which will allow me to confirm the accuracy of my decisions. This type of data analysis was ideal for qualitative case studies (Yin, 2014).

The plan was to use the established interview questions as a guide. Interviews are one of the most powerful methods of qualitative data collection (Polit and Beck, 2012). Researchers can elicit rich information from their participants in this intimate setting. The interviews are interactive, and thus, a researcher can adapt the questions and draw out more information than a survey. Additionally, as a researcher, I actively analyzed the data as the participants are speaking which is the first step in data analysis.

The second step in data analysis was to classify the participants. The classification process includes noting the type of business, the participant role, the participant experience level, and any other characteristics I deemed useful during this process. The third step will be to code the data. Coding involved categorization the data from the interview as it related to the problem statement, purpose statement, and interview questions (De Casterle, Gastmans, Bryon, & Denier, 2012).

To optimize the data collection and coding process, I used the qualitative data analysis software MAXQDA. To utilize MAXQDA, I transcribed the interview questions and answered into Microsoft Word. I ensured the information did not contain participant names or company names. I utilized aliases to protect the identity of the companies and to ensure no harm. Once complete I verified the responses for accuracy and then uploaded the data into MAXQDA to identify any emerging themes and to facilitate coding (De Casterle et al., 2012). I triangulated the data by reviewing and comparing my findings against academic and industry sources.

Reliability and Validity

Reliability

It was important to me as a researcher to convey trust and reliability to your readers. According to Houghton, Casey, Shaw, & Murphy (2013), there are four common components used to assess the reliability and rigor of qualitative data: credibility, dependability, confirmability, and transferability. Additionally, the reliability can be confirmed when the results of the study can be repeated (Darawsheh, 2014). Ali and Yusof (2011) similarly defined reliability as the ability to show consistency and stability throughout responses in a sample population.

To establish credibility and dependability, I utilized member checking in which I had participants review the interview transcription data (Houghton et al., 2013). Additionally, I provided a debriefing to all participants and gave them the results of the study (Thomson, Petty, Ramage, & Moore, 2011). To establish confirmability and dependability in this study, I documented the criteria selection for participants, the overarching research question, and the participant interview questions. Documenting the questions provides an audit trail for mapping responses to similar questions (Houghton et al., 2013). Furthermore, the depth and breadth of detail allow the reader to form a holistic view of the research, building transferability of the study.

Validity

Reliability and validity are the cornerstones of research. Researchers use reliability techniques to verify that the tool is stable and produces consistent results, and validity to ensure the test measures what it is purported to measure (Köksal, Ertekin, Çolakoglu, 2014). It was important to me as a researcher to depict the intent of the study to the participants (Zamanzadeh, Jasemj, Valizadeh, Keogh, & Taleghani, 2015) accurately.

Qualitative research data validity encompasses some things. One of the main components of data validity in qualitative research is the honesty of the participant (Lub, 2015). Also, the accuracy of the data transcription by the researcher must be precise and capture the sentiments of the participants (Thomas & Magilvy, 2011). One of the first steps a researcher can take to ensure validity is data saturation (Guest, Brunce, & Johnson, 2006). Data saturation is when no new data or information is needed, no new coding or themes, and the study is replicable (Guest et al., 2006; Walker, 2012).

Once researchers sample an appropriate size, they often validate the findings through a technique called member checking. Member checking is the process in which the participant validates the researcher's transcription to ensure it is accurate (Houghton et al., 2013). Member checking lends credibility, reliability, and validity to the study through participate verification (Leedy & Omrod, 2013). I allowed members to review their interview transcripts for accuracy. Also, I triangulated data to ensure patterns and themes aligned with academic and industry sources.

Transition and Summary

The purpose of Section 2 was for me to describe my role as a researcher, my experience with cyber-security, and define the participants of the study. I described the steps I am taking to ensure I am compliant with Walden University's ethical standards. Additionally, in Section 2 I described the participants of the study and described the research method and design. I explained how I will utilize a case study approach and how that will allow me to target small businesses and their specific interactions with cyber-security controls. I discussed how I would utilize methodological data triangulation to corroborate findings. Finally, I discussed data reliability and validity techniques I will utilize to ensure alignment between my findings and the intent of the interviewee. Section

3 will include details on the findings of the research, implications for social change, and recommendations for further research.

Section 3: Application to Professional Practice and Implications for Change

Introduction

The purpose of this qualitative multiple case study was to explore strategies used by small business owners to make informed decisions for cyber-security investments to protect the business from cyber-attacks. One of the biggest issues a company, whether large or small, must face is defending themselves against cyber-attacks (Fielder, Panaousis, Malacaria, Hankin, & Smeraldi, 2016). I administered eight semi structured interview questions to the participants to extract information regarding their personal experience and opinions regarding the research topic (Marshall & Rossman, 2016). Also, I reviewed and evaluated academic and commercial literature as part of the data collection for this study. The results of the study aligned with the literature reviewed.

I utilized MaxQDA as a qualitative data analysis tool. I transcribed my interviews into Microsoft Word and imported the results into MaxQDA as individual interviews. Doing so enabled me to identify patterns and themes. In addition to the coded data, I utilized the data analysis, and methodological triangulation to identify emergent themes within the data related to; strategies used by small business owners to make informed decisions for cyber-security investments to protect the business from cyber-attacks. The five central themes that emerged were: government requirements, peer influence, budgetary constraints, commercial standards, and lack of employee involvement.

Presentation of the Findings

The central research question was: What strategies do small business owners use to make decisions regarding cyber-security investments? Ten small business owners participated in the study. To participate, the businesses must have been classified as a small business according to the criteria established by the U.S. SBA specific to their North American Industry, reside in the southeastern United States, had been in business at least one year, and had not had a cyber-security breach in the last 12 months.

The interviewees answered eight semi structured questions designed to capture what influenced their decisions regarding cyber-security investments. The interviews were tape recorded and then manually transcribed into Microsoft Word. Once the transcription was complete, I asked the participants to verify I adequately conveyed their thoughts. Member checking is a vital component of qualitative research (Carlson, 2010). I then imported the transcripts into MaxQDA and began analyzing the data in search of common themes.

The central themes that emerged were; government requirements, peer influence, budgetary constraints, commercial standards, and lack of employee involvement. Table 1 includes descriptions and examples for each theme. I then further developed the themes through recognition of interconnection to other themes, and regularity or frequency of occurrence (Moustakas, 1994). The following sections present summaries of each theme.

Table 1

Emergent Themes

Theme	Description	Examples
Government requirements	Comments about imposed government, regulatory, statutory, or legal requirements	Small business owners must implement cyber-security requirements to operate.
Peer influence	Comments about aligning with peers to stay competitive	To stay competitive, small business owners purchase the latest and greatest technology and cyber-security solutions.
Budgetary constraints	Comments about costs associated with cyber-security protection	Emerging requirements are becoming increasingly expensive and are non-billable to customers.
Commercial standards	Comments about implementing commercial standards for a competitive edge	Small business owners feel the pressure to implement the costly commercial standard to stay competitive with their peers.
Lack of employee involvement	Comments about employees not being a part of the overarching cyber-security solution	Employees are not part of the overall cyber-security solution for small businesses and do not require consideration.

Theme 1: Government Requirements

The first theme, government requirements, emerged during the first two interview questions which focused on assessing their current cyber-security strategies and what resources were small business owners used. The questions were: What strategies are you using to secure your business from cyber-security attacks? And What type of resources did you use to craft your cyber-security strategies? Of the 10 participants, 6 (60%) responded that their major influence when making cyber-security decisions for their business was related to regulatory or legal requirements imposed by the United States Government on their business. The other 4 (40%) indicated their cyber-security policy decisions did not pertain to government regulations rather a mixture of customer requirements or peer influence.

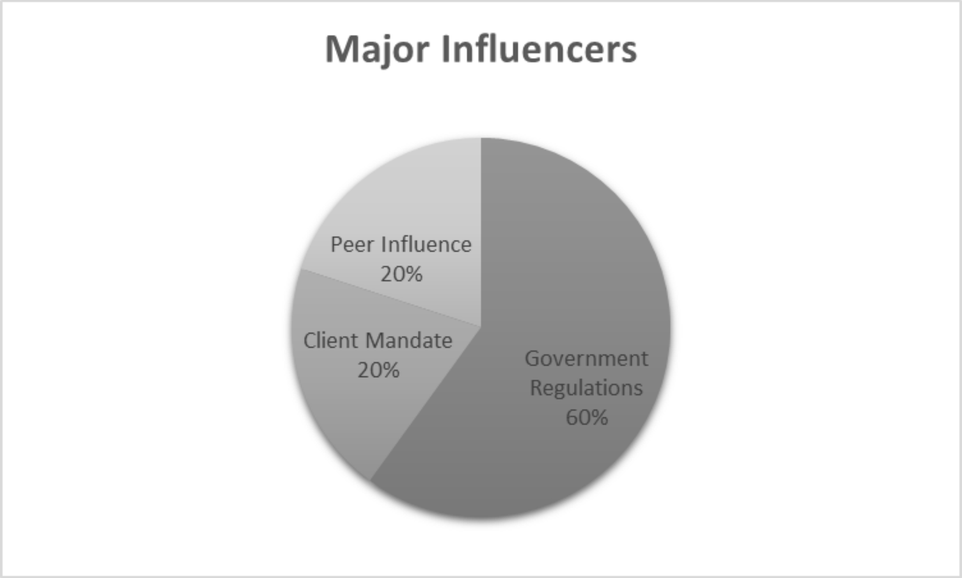

Figure 1. Cyber-security influencers. Major influencers regarding cyber-security policy decisions.

This theme included regulatory requirements that were specific to the type of work that the customer performed. For example, government contractors were required to implement more stringent requirements than commercial businesses. Additionally, small business owners spoke off government imposed standards. These standards were specific to the industry of the business. If the small business was in the financial industry, they had to implement government imposed financial standards. Lastly, small business owners referenced legal requirements. These requirements were specific to the type of data the customer handled.

Participants spoke about crafting their cyber-security strategy against the requirements various entities had prescribed for them. The requirements vary based on the type of business, as well as in complexity, which some participants indicated was increasing. Participant 1 contented:

> Information security used to be an afterthought to me until it was forced upon me by the government. I had a virus scanner and pretty much relied on the vendors for security. Now, I have to make a conscious effort to implement the controls the government has given me or I don't work.

In the last decade, cyber-security has emerged as a top priority for both government and industry (Bashir, Wee, Memon, & Guo, 2017). To an extent, cyber-security is becoming granular, increasingly complex, and costly. Government imposed governance can vary based on industry, data types, and NAIC code. Participant 4 explained, "I do what the government tells me which is getting worse each year." At the time of the interview, the participant was in the midst of implementing a complex set of security controls. The security controls encompassed their entire network and required a significant monetary investment.

Table 2 is a depiction of the common phrases and detected patterns that made up this theme. The common themes that emerged indicated that many of the participants implemented what was required of them by the government to legally operate their business. The remainder of the participants made cyber-security policy decisions that were peer influenced or customer driven. Ultimately, all influencers related to small business owners making cyber-security policy decisions during the course of regular business.

Table 2

Government Influencers

Theme	Description	Examples
Regulatory Requirements	Comments about regulatory requirements specific to the type of work the business is engaged in	The government imposes new regulatory requirements to keep pace with emerging threats.
Government Standards	Comments about complying with standards the government has established for an industry	The government has standards to abide by to do business.
Legal Requirement	Comments about legal requirements for the type of data the business handles	The government has imposed legal requirements that must be adhered to before a company can legally do business.

Theme 2: Peer Influence

The second theme, peer influence, embodied the small business owners' reliance on industry trend analysis, and peer influence. Of the 10 participants, 9 (90%) described their reliance on keeping up with external influencers. These influencers tie back to being a business differentiator. A business differentiator being something that makes that business marketable or more competitive in their particular market. Participant 4 said, "In order to stay competitive, or be allowed to work in this industry, I have to be just as good as the next guy."

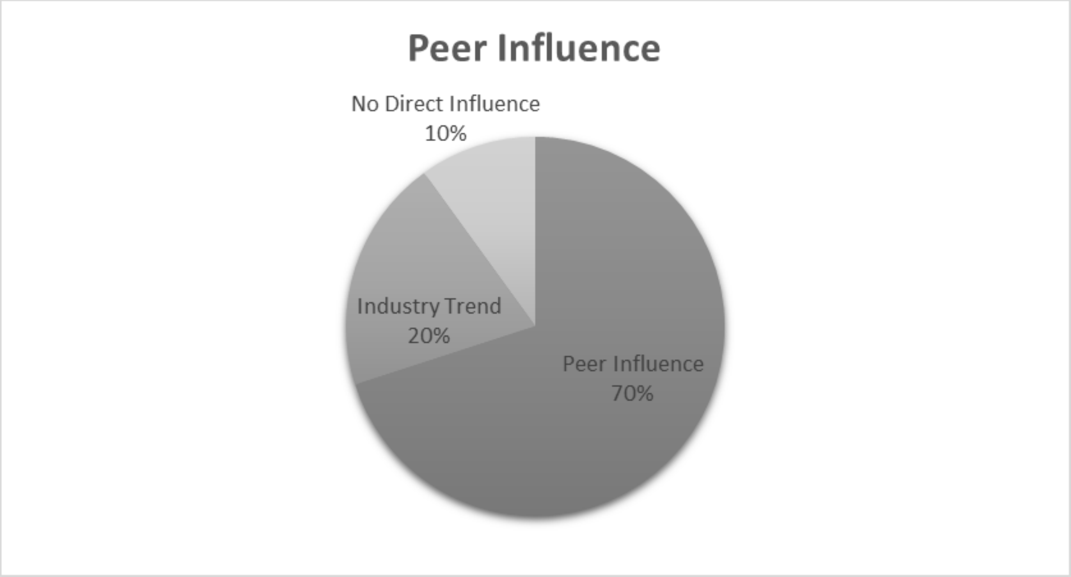

Figure 2. Peer influencers*.* Small business owners indicated their main influencers are peers are industry trends.

These external influences presented in several diverse ways to include in the form of advanced cyber-security techniques 2 (20%), additional hardware or point of sale technology 5 (50%), or additional software investment 2 (20%). Additionally, Participant 10 said, “with a new generation of millennials who like everything fast and flashy, I have to keep up.” Upgrades are costly, but it's something I have learned to budget for now because every upgrade brings more bells and whistles and presumably, more security (Participant 4).

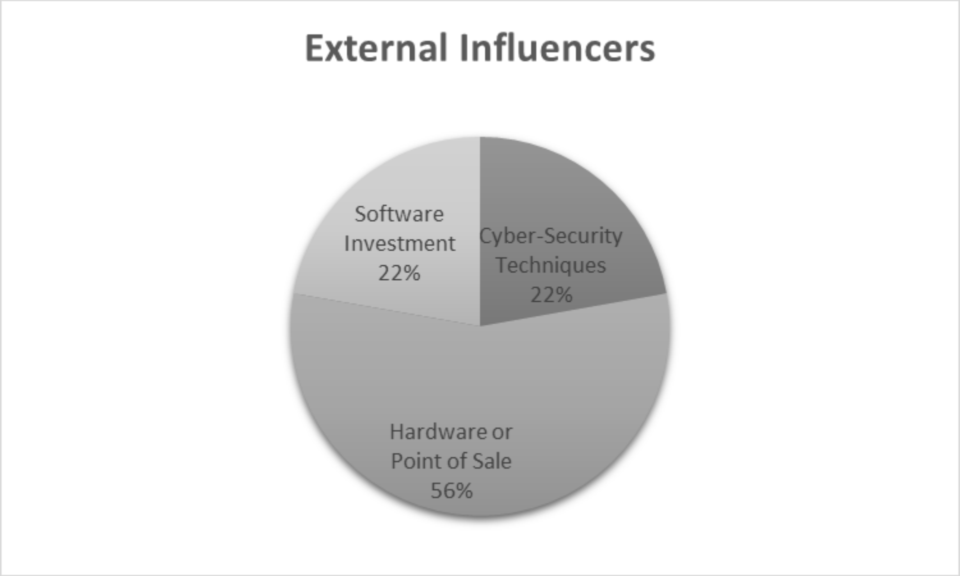

Figure 3. External influencers. External influencers that drive small business owner cyber-security policy decisions.

Participant 1 stated, “we are told what to do by the government but to be competitive, we have to go a step further. Usually, that requires an external certification.” Standards like ISO 27001 and COBIT provide users with a framework to follow based on industry best practices but do not dictate specific requirements (Hoy & Foley, 2015). While certifications are a business differentiator, they are also a way to keep up with the ever-changing requirements (Participant 8).

Table 3 is a depiction of the common phrases and detected patterns that made up this theme. The common theme that emerged here was that small business owners now view cyber-security as an area that they must remain competitive with other businesses. Only one of the ten respondents did not share this sentiment. The data collected suggests that consumers are looking for cyber-security in their products, such as certifications or new hardware. With this expectation comes a greater need to implement industry standard solutions.

Table 3

External Influencers

Theme	Description	Examples
Cyber-Security Techniques	Comments regarding implementing optional cyber-security techniques	Implementing some of the more advanced cyber-security techniques allow businesses to stand out.
Hardware or POS technology	Comments regarding implement hardware or POS sale technology as a differentiator	Implementing the latest hardware or point of sale technology stands out to our customer base.
Additional software investments	Comments regarding spending additional funds on optional software	Implementing advanced software solutions with a flashy interface is familiar and appealing to our customer base.

Theme 3: Budgetary Constraints

The third theme, budgetary constraints, presented throughout each of the interview questions. Of the participants, 10 (100%) indicated that their cyber-security strategy involved budgetary constraints. This theme encompasses the different ways rising costs hamper cyber-security policy decisions. Specifically, through the realization of increasing requirements, disproportioned requirements, the rapid evolution of technology, and the inability recoup security costs.

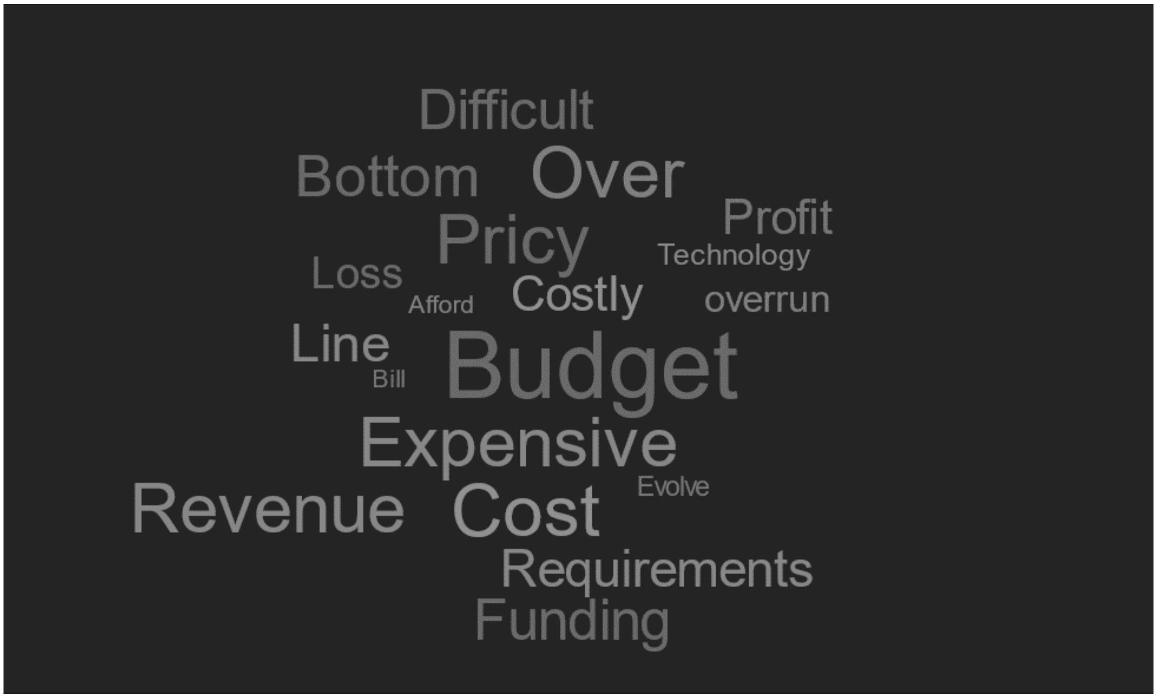

Figure 4. Budgetary constraints. Text cloud of open-ended responses regarding budgetary constraints

When speaking about budgetary constraints, 8 (80%) of the participants mentioned the increase in cyber-security requirements. The requirements can come from their customer, government, or regulatory bodies. Additionally, the requirements can be assumed, meaning they are assuming a need to change their cyber-security posture to accommodate a particular audience. According to Participant 2, “the increase in requirements is fluid and does not seem to cease.”

According to 3 (30%) of the participants, the United States Government requires businesses, regardless of size, but specific to data handling to institute a series of costly and difficult security controls on their corporate network. Small business owners do not have the same access to capital that large businesses have (Dilger, 2017) thereby making new requirements burdensome. According to Participant 4, these requirements are not tailorable and equally enforced regardless of revenue. Furthermore, Participant 6 stated, we do not have large business capital to implement these requirements, but we cannot continue to do business without making these changes. The inability to stay competitive or compliant is significant as it has long term implications for the sustainability of small businesses.

Participant 9 stated, “I don’t have the money to invest in the kind of technology that is needed to be safe.” Moreover, Participant 6 stated, “Sometimes I have to make difficult decisions not to invest in what I know I need.” Further supporting this theme, researchers have called on the academic community to provide additional research and resources to develop cost effective ways to secure the data of small and medium businesses (Gordon et al., 2015; Harris & Patten, 2014).

The ability for small businesses to not only sustain but to keep up with evolving technology is a concern (McDowell, Harris, & Geho, 2016; Pirta & Strazdina, 2012; Theyel & Hofman, 2012). Of the participants interviewed, 5 (50%) discussed the constant evolution of technology and the impact that has on cyber-security and their budgets. Participant 10 stated, “as soon as I get something new, I already see advertisements for the next generation.” This constant turnover is not consistent with technology and business investitures of the past. Rather, small business owners must incorporate these changes as quickly as they appear to stay relevant, and secure.

The rapid changes in technology and requirements leave the small business owner with mounting costs with little room to pass that cost onto the customer. According to 6

(60%) of the participants interviewed, very little of the cost related to cyber-security can be added to the cost of the product leaving the small business owners in a bind on how to recoup that cost. You can only do what you can afford to do, and that could mean lesser profit, staff, or cutting corners on requirements (Participant 8).

Table 4 is a depiction of the common phrases and detected patterns that made up this theme. All participants indicated that cyber-security is costly to small businesses. Also, the participants indicated that cyber-security is a requirement and a differentiator, yet it is not something that they build into the cost of the product or service.

Table 4

Budgetary Constraints

Theme	Description	Examples
Increasing requirements	Comments regarding increasing requirements both from government and end users	A small business owner must account for at least one major change a fiscal year.
Disproportioned requirements	Comments regarding government regulations that are more appropriate for big business	The requirements set forth are not accommodating to small business owners.
Rapid evolution of technology	Comments regarding the rate at which technology changes and the inability to fund these changes	Technology is changing at a far more rapid pace than it has for decades before now.
Inability to incorporate cost into product	Comments regarding the inability to increase product or service costs to cover additional security requirements	The increase costs for cyber-security that cannot be incorporated into the cost of the product.

Theme 4: Commercial Standards

The fourth theme, commercial standards, describes the dependency that the small business owners described having on vendors as opposed to internal staff. Of the ten participants, 9 (90%) indicated that their cyber-security strategy involved utilizing commercial standards, to include software or hardware, and relying on the vendor to integrate security into the product. Participant 2 best summarized this them with, "I expect security to be built into products."

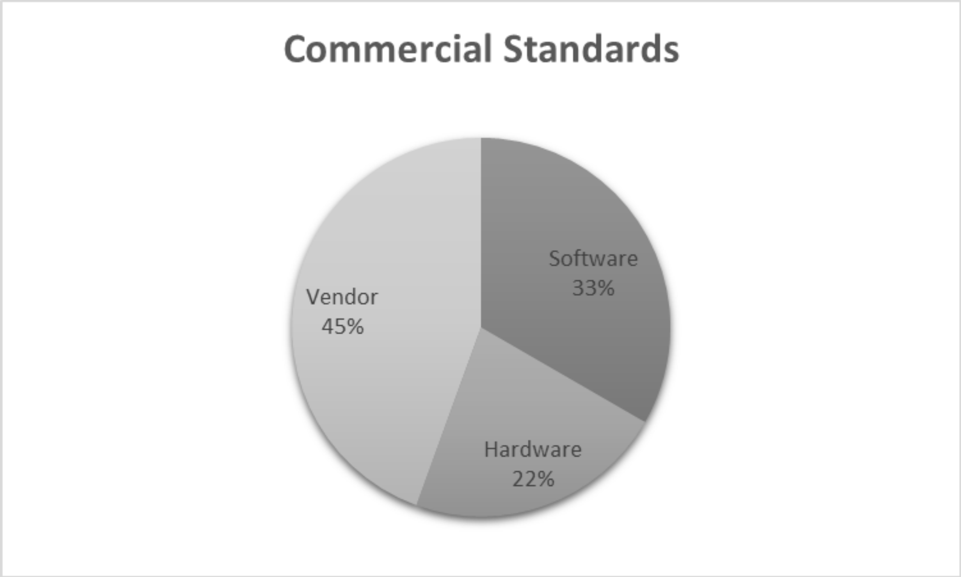

Figure 5. Commercial standards. Small business owner dependency on commercial standards.

Each of the nine participants who indicated they utilized commercial products indicated that they did so because they believed the product came ready to use. Of those nine, eight specifically recalled software or hardware that they purchased solely for the built-in security. None of the nine participants had made any additional changes to the products. According to Interview Participant 5, “I solely rely on Cox communications business suite to secure my business. I use it as is.” Also, Participant 7 stated, “if it wasn’t for commercial software like QuickBooks, I am not sure what I would do.”

Multiple participants, 5 (50%), expressed their willing dependency on Microsoft to meet a large majority of their business needs. Participant 9 stated, “…Office 365 is well known, cheap, and easy to use.” Participant 10 furthered supported that statement by saying, “We utilize Microsoft Office 365 because it is familiar to our employees, and security is intuitive.”

Traditionally, small businesses are slow to adopt technology unless it is familiar or intuitive (Nguyen, Newby & Macaulay, 2015). Of the participants interviewed, 5 (50%) relied on a consultant to implement any additional changes or interpret complex requirements. Participant 10 stated, “I cannot afford someone on staff full time with the type of skill-set required to maintain these requirements.”

Table 4 is a depiction of the common phrases and detected patterns that made up this theme. The common themes that emerged indicated that many participants indicated they were dependent on product vendors to incorporate cyber-security into their product which is not limited to a software or hardware product. It also includes more complex business solutions such as web portals, smart phone applications, and business infrastructure. One participant did not specify that they required cyber-security be built into their products. This could be because their primary business offering is placing employees in open positions at other companies.

Table 5

Commercial Standards

Theme	Description	Examples
Commercial software or hardware solutions	Comments regarding purchasing software or hardware specifically to utilize an integrated security component	It is important to evaluate each hardware or software purchase to determine if it meets stringent security requirements.
Vendor integrated security	Comments about utilizing a vendor to integrate security into software or hardware	The vendor is expected to integrate some degree of security into their product.
Cyber-security Consultants	Comments about using consultants to implement required security components into hardware or software solutions	Consultants often can translate security requirements into actual investments.

Theme 5: Lack of Employee Involvement

The final theme, lack of employee involvement, presented when I asked small business owners about the role their employees played in their cyber-security strategies. Of the ten participants, 7 (70%) indicated that their strategy did not involve their employees at all. Specifically, 3 (30%) said there was no planning for employee training developing cyber-security policies and the other (40%) assumed employees came equipped to perform their job functions securely. The remaining participants incorporated their employees in their policies in one form or another.

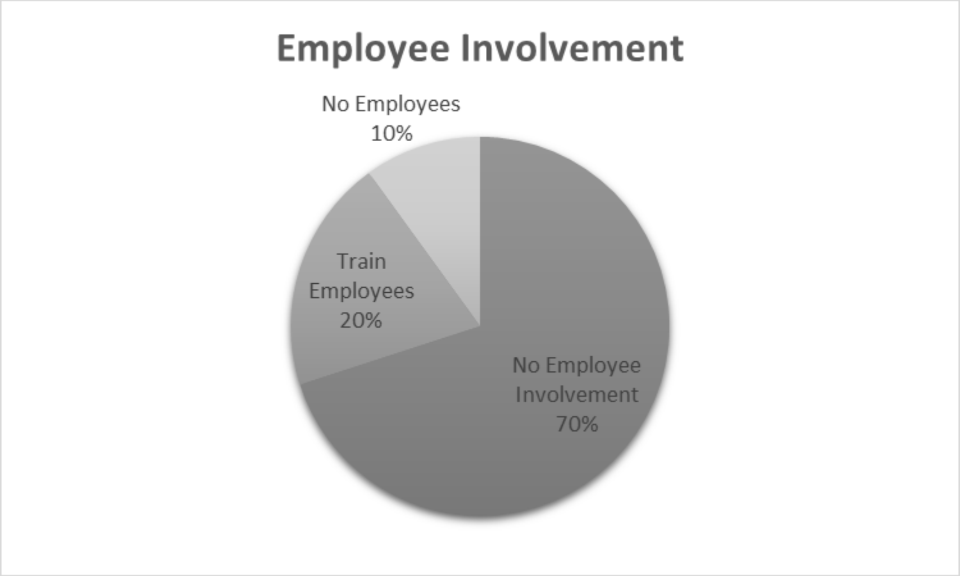

Figure 6. Employee involvement. Summary of employee involvement in cyber-security strategies.

The participants who did not consider their employees when developing cyber-security policies believe their employees have no influence or role in their policy strategies. Participant 4 stated, “I have never thought my employees needed training.” Small business owners can be particularly susceptible to insider threat because they often have access to data from larger entities as part of a teaming agreement and lack sophisticated detection methods (Heidenreich & Gray, 2014). Furthering this theme, Participant 3 stated, “employees don’t play a big role unless they are in the IT department.”

In contrast, some interview participants believed that their employees were part of their overarching cyber-security strategy. These participants believed that all employees came sufficiently trained to play a positive role in their strategy. The belief was that employees utilized technology daily and security should be second nature. The Association of Certified Fraud Examiners found that only 18.5% of small business employees received training in fraud detection and prevention (Tysiac, 2012). Interview Participant 6 stated, "…security should be common sense to them" when speaking of their employees. Additionally, Participant 4 stated "I expect them to know how to use technology securely. It is not my job to educate them on stuff they use every day."

While employees naturally anticipate the need to handle certain data such as financial information securely, cyber-security is not always intuitive (Han, Kim, & Kim, 2016). Participant 7 stated, "Security should be common sense by now." Moreover, Participant 8 stated, "I do not train them. I know no more than they do." Adding, "In the world, we live in, they should know it (Participant 8).

Table 6 is a depiction of the common phrases and detected patterns that made up this theme. Most respondents indicated that they did consider their employees when planning or executing their cyber-security strategies. The lack of employee involvement was evident in the fact that they did not train their employees on any topic related to cyber-security. The respondents that did include employees indicated they did because their customer required it or the product they purchased had security features.

Table 6

Lack of Employee Involvement

Theme	Description	Examples
No specific employee training	Comments about not incorporating cyber-security employee training into policy decisions	The consideration for a secure business depends solely on the network infrastructure, not the users.
Assumed knowledge	Comments about employees already being aware of cyber-security	The assumption that a consideration for employment is security knowledge.

Applications to Professional Practice

Technology continues to progress faster than anyone could have anticipated. With those changes come a plethora of cyber-security threats and vulnerabilities. These threats and vulnerabilities leave small business owners susceptible to damage to their reputation and significant monetary loss. It is critical to identify effective and repeatable methods for small business owners to establish cyber-security policies.

Participants in this study indicated their policy decisions mainly relied on necessity, budgetary constraints, and competitiveness. Additionally, the small business participants indicated they were reliant on commercial vendors to integrate security into their products or consultants to implement complex requirements. Adding that they invested little to no consideration into considering their employees when developing their cyber-security strategies. The most significant contribution this study will have for professional practice is identifying gaps in existing literature. Specifically, existing literature does not identify repeatable methods for scaling and implementing policies that are cost effective and pertinent to typical small business owners.

Moreover, this study may fill gaps in knowledge regarding how small business owners make decisions when cultivating cyber-security policies. As well, it provides current, and future small business owners insight into strategies that are effective as well as areas they should focus on that was previously unknown to them. Furthermore, it provides a more dynamic view into how cyber-security plays a more robust role in day-to-day operations than previously thought.

The results of this study apply to all small business owners who utilize any form of technology in their business activities. I provided a deeper understanding of current literature surrounding cyber-security policy decisions in small businesses as well as real world experiences of current small business owners. The results of the study provide a holistic view of what is working for small business owners and the obstacles they encounter.

Implications for Social Change

Cyber-security attacks targeting small businesses increase from year to year (Rahman & Lackey, 2013), with each breach estimated to cost $263,000 (Symantec, 2016). The estimated cost of a single breach is enough to bankrupt most small businesses. This research could positively contribute to social change by helping small business owners to identify the need for cyber-security strategies. This could, in turn, lend to the overall sustainability of small businesses.

Knowledge gained from this study could influence small business owners to adopt cyber-security strategies they had not previously considered. Cyber-security strategies that interviewees shared during this study may benefit small business owners include utilizing commercial products that already incorporate security. The strategy to utilize products that are affordable, and effective, may increase the security posture of existing small businesses. Also, profitability may increase if the small business owner can cut existing, burdensome costs.

This study could also prompt small business owners to plan for cyber-security costs that they may not have previously considered which could lead to the sustainability of small businesses. Furthermore, small business owners who are considering expanding their service offerings will now consider regulatory, legal, or other statutory requirements and potential costs. These considerations could lead to sustainability and lower the failure rate of small businesses.

Recommendations for Action

During this study, one hundred percent of the participants indicated they could not afford the costs associated with effective cyber-security strategies regrettably cyber-security threats continue to evolve and grow. With over 430 million new unique pieces of malware detected in 2015, which is a 36% increase from 2014 (Symantec, 2016), small business owners must take decisive action to secure their business. Current and future small business owners should understand the importance of effective and sustainable cyber-security strategies. The following recommendations may assist small business owners craft cyber-security policies.

First, small business owners should invest in training their employees. The reliance on employees to be self-sufficient, or come with the appropriate level of knowledge to effectively contribute to their overall cyber hygiene is not realistic. Small business owners should take advantage of free or reduced cost training resources offered by the vendor or the government. Doing so would greatly increase the effectiveness of their cyber-security strategy.

Second, small business owners should be more vocal in expressing their need for government assistance as it relates to evolving regulations. I recommend that small business owners band together and deliver an impact statement to the regulatory board for complex regulations that are the most burdensome. Also, when regulations are in their comment phase, small business owners should coordinate with the SBA to ensure their concerns are adequately captured and conveyed.

My last recommendation is for small business owners to form an online community specifically designed to share lessons learned regarding cyber-security. While there is a multitude of websites focused on cyber-security they are more marketing focused. Small business owners need a place where they can share what worked for them or ask questions of other small business owners. The best perspective comes from those who share similarities and common traits.

Recommendations for Further Research

The purpose of this qualitative multiple case study was to explore strategies used by small business owners to make informed decisions for cyber-security investments to protect the business from cyber-attacks. Ten small business owners participated from the

Southeastern United States. To participate, the small business owners had to have been in business for a least a year, and not had a cyber-security breach in the last 12 months.

The results of the study indicated that small business owners limited their cyber-security strategies to government regulations or what using commercial products that have security protections in place. Additionally, small business owners indicated that their budgets limited their policy decisions. Furthermore, small business owners indicated they did not involve their employees in decisions regarding policies or strategies.

The first recommendation for further research is to perform a quantitative study aimed at establishing a robust security program. A quantitative study could give small business owners insight into the potential cost of cyber-security policy decisions as it relates to the potential impact on their business. Additionally, the study could quantify the benefits of cyber-security policies.

My second recommendation for further research is to conduct a quantitative study that assesses the specific risk for each participating business versus the security controls in place. An additional quantitative study could begin to address the potential limitation that small business owners may inadvertently provide inadequate data due to their limited knowledge of cyber-security. Essentially, this study has the potential to establish a baseline set of required controls as opposed to what is in place. Furthermore, a quantitative study of this nature would produce results that could either justify the lack of controls in place or the need for more.

My final recommendation for further research is to perform a larger qualitative study with the intent of reaching a considerably larger population. The qualitative study could have a similar structure, but instead of in-person interviews, the researcher could utilize an online survey. An online survey could reach a broader audience and give researchers insight into new, effective strategies. Also, the anonymity of an online survey may produce a deeper breadth of answers.

Reflections

With over 20 years of industry experience, I am considered a subject matter expert in my field. I am often called upon to author policies or verify the efficiency of existing policies. When I started this journey, I chose a topic that I believed warranted further exploration due to current trends in information security. To reduce the potential for personal bias, I selected small business owners as my primary focal point since my primary experience is with a large business or government entities.

When I began my research, I did not have any preconceived notions of what influenced small business owners when making cyber-security policy decisions. In my review of existing literature, I found that small business owners were as much of a target, if not more, as big business or government entities. I also found that there were limited qualitative studies that involved actual small business owners in assessing what they had in place.

The interviews were educational and eye opening. While I am familiar with budget constraints, I had not fully contemplated how much cyber-security affected small business owners. Moreover, I have an appreciation for the role of a small business owner. They do not have a large cadre of people to assist in making decisions. They rely on their own experience and ability to research and understand complex topics.

Conclusion

The purpose of this qualitative multiple case study was to explore the strategies small business owners use to make cyber-security decisions. Ten small businesses in the Southeastern United States participated in this study. I employed semi structured interviews to provide answers to my research question. The research question was: What strategies do small business owners use to make decisions regarding cyber-security?

Five themes occurred: government requirements, peer influence, budgetary constraints, commercial standards, and lack of employee involvement. According to the participants, budgetary constraints and peer influence were the most influential factors when making decisions regarding cyber-security strategies. The emergent themes aligned with the literature review and conceptual framework of this study.

Cyber-security has gone from an afterthought to a necessity. The rapid evolution and adoption of technology coupled with the growing threat base have made cyber-security something small business owners must consider. Proper planning and continuous review of cyber-security strategies are essential to the sustainability of small businesses. I recommend that small business owners, scholars, and practitioners use the results of this study to gain insight into effective decision-making strategies and expand on these strategies until they find a long-term, sustainable solution.

References

Ahmad, R., & Yunos, Z. (2012). The application of mixed method in developing a cyber terrorism framework. *Journal of Information Security*, *3*(3), 209-214. Retrieved from http://www.scirp.org/journal/jis/

Akhtar, N., Azeem, S., & Mir, G. (2014). Strategic role of internet in SMES growth strategies. *International Journal of Business Management & Economic Research*, *5*(2), 20-27. Retrieved from http://www.ijbmer.com/

Alhogail, A., & Mirza, A. (2014). A framework of information security culture change. *Journal of Theoretical & Applied Information Technology, 64*, 540-549. Retrieved from www.jatit.org

Anderson, C. A., Leahy, M. J., DelValle, R., Sherman, S., & Tansey, T. N. (2014). Methodological application of multiple case study design using modified consensual qualitative research (CQR) analysis to identify best practices and organizational factors in the public rehabilitation program. *Journal of Vocational Rehabilitation*, *41*, 87-98. http://dx.doi.org/10.3233/JVR-140709

Ates, A., & Bititci, U. (2011). Change process: a key enabler for building resilient SMEs. *International Journal of Production Research*, *49*, 5601-5618. http://dx.doi.org/10.1080/00207543.2011.563825

Avgerinos, T., Sang Kil, C., Rebert, A., Schwartz, E. J., Woo, M., & Brumley, D. (2014). Automatic exploit generation. *Communications of the ACM*, *57*(2), 74-84. http://dx.doi.org/10.1145/2560217.2560219

Ban, H. J., Choi, J., & Kang, N. (2016). Fine-grained support of security services for resource constrained Internet of Things. *International Journal of Distributed Sensor Networks*, 1-8. http://dx.doi.org/10.1155/2016/7824686

Bandar, B. M., & Christian, B. (2013). Perceived risk of information security and privacy in electronic commerce. *International Journal of Advanced Research in Computer Science, 8*. Retrieved from http://www.ijarcce.com/

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

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

Beckers, K., Côté, I., Faßbender, S., Heisel, M., & Hofbauer, S. (2013). A pattern-based method for establishing a cloud-specific information security management system. *Requirements Engineering*, *18*(4), 343-395. http://dx.doi.org/10.1007/s00766-013-0174-7

Bekhet, A. K., & Zauszniewski, J. A. (2012). Methodological triangulation: An approach to understanding data. *Nurse Researcher*, *20*(2), 40-43. http://dx.doi.org/10.7748/nr2012.11.20.2.40.c9442

Bernik, I. (2014). Cybercrime: The cost of investments into protection. *Varstvoslovje: Journal of Criminal Justice & Security*, *16*(2), 105-116. Retrieved from http://www.fvv.uni-mb.si/rV/revija-E.html

Borrajo, M. L., Baruque, B., Corchado, E., Bajo, J., & Corchado, J. M. (2011). Hybrid neural intelligent system to predict business failure in small-to-medium size enterprises. *International Journal of Neural Systems*, *21*, 277-296.

http://dx.doi.org/10.1142/S0129065711002833

Borrett, M., Carter, R., & Wespi, A. (2013). How is cyber threat evolving and what do organisations need to consider. *Journal of Business Continuity & Emergency Planning*, *7*(2), 163-171. Retrieved from http://www.henrystewartpublications.com/jbcep

Branker, J., Eveleigh, T., Holzer, T. H., & Sarkani, S. (2016). Access control, identity management and the insider threat. *Journal of Airport Management*, *10*. Retrieved from www.henrystewartpublications.com/jam

Breaux, R. W., Black, E. W., & Newman, T. (2014). A guide to data protection and breach response. *Intellectual Property & Technology Law Journal*, *26*(7), 3-10. Retrieved from http://www.intellectualpropertylaw.tv/

Brenner, J. D. (2013). Eyes wide shut: The growing threat of cyber attacks on industrial control systems. *Bulletin of the Atomic Scientists*, *69*(5), 15-20. Retrieved from http://www.tandfonline.com

Britton, K. (2016). Handling privacy and security in the internet of things. *Journal of Internet Law*, *19*, 3-7. Retrieved from https://lrus.wolterskluwer.com/

Cader, H., & Leatherman, J. (2011). Small business survival and sample selection bias. *Small Business Economics*, *37*, 155-165. http://dx.doi.org/10.1007/s11187-009-9240-4

Carlson, J. A. (2010). Avoiding traps in member checking. *Qualitative Report*, *15*(5), 1102-1113. Retrieved from http://www.nova.edu/ssss/QR/QR15-5

Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J., & Neville, A. J. (2014). The use of triangulation in qualitative research. *Oncology Nursing Forum*, *41*(5), 545-547. http://dx.doi.org/10.1188/14.ONF.545-547

Cezar, A. (2013). Outsourcing information security: Contracting issues and security implications. *Management Science*, 638-657. http://dx.doi.org/10.1287/mnsc.2013.1763

Chauhan, S., & Panda, N. (2015). Hacking web intelligence. *Network Security, 2015*. http://dx.doi.org/10.1016/S1353-4858(15)30066-0

Choucri, N., Madnick, S., & Ferwerda, J. (2014). Institutions for cyber security: International responses and global imperatives. *Information Technology for Development*, *20*(2), 96-121. http://dx.doi.org/10.1080/02681102.2013.836699

Clinton, L. (2015). Best practices for operating government-industry partnerships in cyber security. *Journal of Strategic Security*, *8*(4), 53-68. http://dx.doi.org/10.5038/1944-0472.8.4.1456

Cohen, D. (2011). Feature: External pressure for internal information security controls. *Computer Fraud & Security, 20118*(8). http://dx.doi.org/10.1016/S1361-3723(11)70113-0

Collins, C. S., & Cooper, J. E. (2014). Emotional intelligence and the qualitative researcher. *International Journal of Qualitative Methods*, *13*(1), 88-103. Retrieved from https://ejournals.library.ualberta.ca/index.php/IJQM/

Collins, K. T., Onwuegbuzie, A. J., Johnson, R. B., & Frels, R. K. (2013). Practice note: Using debriefing interviews to promote authenticity and transparency in mixed research. *International Journal of Multiple Research Approaches*, *7*(2), 271-284.

http://dx.doi.org/10.5172/mra.2013.7.2.271

Conrad, J. (2012). Seeking help: The important role of ethical hackers. *Network Security*, *2012*(8), 5-8. http://dx.doi.org/10.1016/S1353-4858(12)70071-5

Currie, W. L., & Seddon, J. M. (2014). Social innovation in public health: Can mobile technology make a difference? *Information Systems Management*, *31*, 187-199. http://dx.doi.org/10.1080/10580530.2014.923263

Darawsheh, W. (2014). Reflexivity in research: Promoting rigour, reliability and validity in qualitative research. *International Journal of Therapy & Rehabilitation*, *21*(12), 560-568. Retrieved from http://www.magonlinelibrary.com/toc/ijtr/current

Davies, A. (2015). Qualitative research in action: A Canadian primer. *Canadian Journal of Action Research*, *16*(3), 79-82. Retrieved from http://cjar.nipissingu.ca/index.php/cjar/index

De Casterle, B. D., Gastmans, C., Bryon, E., & Denier, Y. (2012). QUAGOL: A guide for qualitative data analysis. *International Journal of Nursing Studies, 49*, 360-371. Retrieved from http://www.journals.elsevier.com/international-journal-of-nursing-studies/

Dey, R., & Sullivan, M. W. (2012). Was Dodd-Frank justified in granting internal control audit exemption to small firms? *Managerial Auditing Journal*, *27*(7), 666-692. http://dx.doi.org/10.1108/02686901211246804

Dinicu, A. (2014). Cyber threats to national security. Specific features and actors involved. *Bulletin Scientific*, *19*, 109-113. Retrieved from http://www.scientificbulletin.upb.ro/

Doyle, C., Howe, C., Woodcock, T., Myron, R., Phekoo, K., McNicholas, C., & Bell, D. (2013). Making change last: Applying the NHS Institute for innovation and improvement sustainability model to healthcare improvement. *Implementation Science, 8*(127), 1-24. http://dx.doi.org/10.1186/1748-5908-8-127

Eastman, J. K., Iyer, R., Liao-Troth, S., Williams, D. F., & Griffin, M. (2014). The role of involvement on millennials' mobile technology behaviors: The moderating impact of status consumption, innovation, and opinion leadership. *Journal of Marketing Theory & Practice*, *22*, 455-470. http://dx.doi.org/10.2753/MTP1069-6679220407

Eisenhardt, K. M., & Graebner, M. E. (2007). Theory building from cases: Opportunities and challenges. *Academy of Management Journal*, *50*. http://dx.doi.org/10.5465/AMJ.2007.24160888

Elie-Dit-Cosaque, C., Pallud, J., & Kalika, M. (2011). The influence of individual, contextual, and social factors on perceived behavioral control of information technology: A field theory approach. *Journal of Management Information Systems*, *28*, 201-234. http://dx.doi.org/doi.org/10.2753/MIS0742-1222280306

Ethala, K., & Seshadari, R. R. (2013). Combating cyber terrorism - assessment of log for malicious signatures. *American Journal of Applied Sciences*, *10*, 1660-1666. http://dx.doi.org/10.3844/ajassp.2013.1660.1666

Everett, C. (2011). Feature: Is ISO 27001 worth it? *Computer Fraud & Security, 20115*(7). http://dx.doi.org/10.1016/S1361-3723(11)70005-7

Everett, C. (2016). Feature: Ransomware: to pay or not to pay? *Computer Fraud &*

Security, *20168*. http://dx.doi.org/10.1016/S1361-3723(16)30036-7

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision Support Systems*. http://dx.doi.org/10.1016/j.dss.2016.02.012

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

Gao, X., Zhong, W., & Mei, S. (2015). Security investment and information sharing under an alternative security breach probability function. *Information Systems Frontier*, *17*, 423-438. http://dx.doi.org/10.1007/s10796-013-9411-3

Georgescu, M., & Suicimezov, N. (2012). Issues regarding security principles in cloud computing. *USV Annals of Economics & Public Administration*, *12*, 221-226. Retrieved from http://www.seap.usv.ro/annals/ojs/index.php/annals

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

Gordon, L. A., Loeb, M. P., & Lei, Z. (2011). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security*, *19*(1), 33-56. http://dx.doi.org/10.3233/JCS-2009-0398

Gordon, L., Loeb, M., Lucyshyn, W., & Zei, L. (2015). The impact of information sharing on cybersecurity underinvestment: A real options perspective. *Journal of Accounting and Public Policy*, *34*, 509-519. http://dx.doi.org/10.1016/j.jaccpubpol.2015.05.001

Guest, G., Brunce, A., & Johnson, L. (2006). How many interviews are enough? An experiment with data saturation and variability. *Field Methods*, *18*, 59-82. http://dx.doi.org/10.1177/1525822X05279903

Gulenko, I. (2014). Improving passwords: Influence of emotions on security behaviour. *Information Management & Computer Security*, *22*, 167-178. http://dx.doi.org/10.1108/MCS-09-2013-0068

Gupta, M., Chaturvedi, A., & Mehta, S. (2011). Economic analysis of tradeoffs between security and disaster recovery. *Communications of The Association for Information Systems*, *28,* 1-16. Retrieved from http://aisel.aisnet.org/cais/

Gupta, P., Seetharaman, A. A., & Raj, J. (2013). The usage and adoption of cloud computing by small and medium businesses. *International Journal of Information Management*, *33*, 861-874. http://dx.doi.org/10.1016/j.ijinfomgt.2013.07.001

Hardicre, J. (2014). Valid informed consent in research: An introduction. *British Journal of Nursing*, *23*(11), 564-567. Retrieved from http://www.magonlinelibrary.com/toc/bjon

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. http://dx.doi.org/10.1108/IMCS-03-2013-0019

Hayes, J., & Bodhani, A. (2013). Cyber security: Small businesses under fire. *Engineering & Technology*, *8*(6), 80-83. Retrieved from http://www.onlinejet.net/

Hayes, T. R. (2012). Predicting information technology adoption in small businesses: An extension of the technology acceptance model. *Academy of Information and*

Management Sciences Journal, *1*. Retrieved from http://www.alliedacademies.org/aimsj_public.php

Heidenreich, B., & Gray, D. H. (2014). Cyber-Security: The threat of the internet. *Global Security Studies*, *5*(1), 17-26. Retrieved from http://www.globalsecuritystudies.com/archives.htm

Hill, C. E., Knox, S., Thompson, B. J., Hess, E. N., & Ladany, N. (2005). Consensual qualitative research: An update. *Journal of Counseling Psychology*, *52*(2), 196-205. http://dx.doi.org/10.1037/0022-0167.52.2.196

Holm, H., Sommestad, T., Ekstedt, M., & Honeth, N. (2014). Indicators of expert judgement and their significance: an empirical investigation in the area of cyber security. *Expert Systems*, *31*(4), 299-318. http://dx.doi.org/10.1111/exsy.12039

Everett, C., (2016). *Network Security*, 1-2. http://dx.doi.org/10.1016/S1353-4858(16)30031-9

Houghton, C., Casey, D., Shaw, D., & Murphy, K. (2013). Rigour in qualitative case-study research. *Nurse Researcher*, *20*(4), 12-17. Retrieved from www.nurseresearcher.co.uk

Hoy, Z., & Foley, A. (2015). A structured approach to integrating audits to create organisational efficiencies: ISO 9001 and ISO 27001 audits. *Total Quality Management & Business Excellence*, *25*, 690-702. http://dx.doi.org/doi:10.1080/14783363.2013.876181

Hui, K., Hui, W., & Yue, W. T. (2012). Information security outsourcing with system interdependency and mandatory security requirement. *Journal of Management*

Information Systems, *29*(3), 117-156. http://dx.doi.org/10.2753/MIS0742-1222290304

Hutchings, A., Smith, R., & Lau, L. (2015). Criminals in the Cloud: Crime, Security Threats, and Prevention Measures. In *Cybercrime Risks and Responses* (II ed. (pp. 146-162). http://dx.doi.org/10.1057/9781137474162_10

Hyman, P. (2013). Cybercrime: It's serious, but exactly how serious? *Communications of The ACM*, *56*(3), 18-20. http://dx.doi.org/10.1145/2428556.2428563

Ibrahim, N. A. (2012). Formalized business planning decisions in small firms. *Journal of International Business Strategy*, *12*(1), 81-86. Retrieved from http://www.iabe.org/domains/iabeX/journal.aspx?journalid=7

Ibrahim, N., & Edgley, A. (*20*15). Embedding researcher's reflexive accounts within the analysis of a semi-structured qualitative interview. *Qualitative Report,* 20(10), 1671-1681. Retrieved from http://www.nova.edu/ssss/QR/index.html

Jacob, S. A., & Furgerson, S. P. (2012). Writing interview protocols and conducting interviews: Tips for students new to the field of qualitative research. *Qualitative Report*, *17*(42), 1-10. Retrieved from http://www.nova.edu/ssss/QR/index.html

Jarvis, L., Macdonald, S., & Nouri, L. (2014). The cyberterrorism threat: Findings from a survey of researchers. *Studies in Conflict & Terrorism*, *37*(1), 68-90. http://dx.doi.org/10.1080/1057610X.2014.853603

Jingguo, W., Gupta, M., & Rao, H. R. (2015). Insider threats in a financial institution: Analysis of attack proneness of information systems applications. *MIS Quarterly*, *39*(1), 91-A7. Retrieved from http://www.misq.org/

Kaynak, O., & Karagöz, N. A. (2014). Experience report: implementation of a multi-standard compliant process improvement program. *Journal of Software: Evolution & Process*, *26*(5), 488-495. http://dx.doi.org/doi:10.1002/smr.1610

Khalaj, M., Makui, A., & Tavakkoli-Moghaddam, R. (2012). Quantitative and qualitative methods in risk-based reliability assessing under epistemic uncertainty. *South African Journal of Industrial Engineering*, 84-96. Retrieved from http://www.scielo.org.za/scielo.php?lng=en

Kinney, J. R., & Shepardson, M. L. (2011). Do control effectiveness disclosures require SOX 404(b) internal control audits? A natural experiment with small U.S. public companies. *Journal of Accounting Research*, *49*(2), 413. http://dx.doi.org/10.1111/j.1475-679X.2011.00400.x

Kivimaa, J. (2013). A cost optimizing model for IT security. *Baltic Journal of Economics*, *13*(2), 137-138. Retrieved from http://www.sseriga.edu/en/centres/biceps/bje/

Köksal, M. S., Ertekin, P., & Çolakoglu, O. M. (2014). How differences among data collectors are reflected in the reliability and validity of data collected by Likert-Type scales? *Educational Sciences: Theory and Practice*, *14*, 2206-2212. http://dx.doi.org/10.12738/estp.2014.6.2028

Lanz, J. (2013). Helping small and midsized businesses succeed in a technology-driven world. *CPA Journal*, 6-9. Retrieved from http://www.cpajournal.com/

Laszka, A., Johnson, B., Schottle, P., Grossklags, J., & Bohme, R. (2014). Secure team composition to thwart insider threats and cyber-espionage. *ACM Transactions On*

Internet Technology, *14*(2), 1-19. http://dx.doi.org/10.1145/2663499

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. H. (2014). Information security awareness and behavior: a theory-based literature review. *Management Research Review*, *37*, 1049-1092. http://dx.doi.org/10.1108/MRR-04-2013-0085

Leedy, P. D., & Ormrod, J. E. (2013). *Practical research: Planning and design* (10th ed.). Upper Saddle River, NJ: Pearson Education.

Lesnykh, A. (2011). Data loss prevention: A matter of discipline. *Network Security*, *2011* (3), 18-19. http://dx.doi.org/10.1016/S1353-4858(11)70028-9

Liao, K., & Chueh, H. (2012). Medical organization information security management based on ISO27001 information security standard. *Journal of Software*, *7*, 792-797. http://dx.doi.org/10.4304/jsw.7.4.792-797

Lub, V. (2015). Validity in qualitative evaluation: Linking purposes, paradigms, and perspectives. *International Journal of Qualitative Methods*, *14*(5), 1-8. http://dx.doi.org/10.1177/1609406915621406

Nicoll, S. R., & Owens, R. W. (2013). Emergency response & business continuity. *Professional Safety*, *58*(9), 50-55. Retrieved from https://www.asse.org/professionalsafety/

Nissim, N., Boland, M. R., Tatonetti, N. P., Elovici, Y., Hripcsak, G., Shahar, Y., & Moskovitch, R. (2016). Improving condition severity classification with an efficient active learning based framework. *Journal of Biomedical Informatics*, *61*, 44-54. http://dx.doi.org/10.1016/j.jbi.2016.03.016

Opara, E. U., & Bell, R. L. (2011). The relative frequency of reported cases by information technology professionals of breaches on security defenses. *International Journal of Global Management Studies Professional, 3*(2), 15-28. Retrieved from http://association-gms.org/index.php/journals/ijgmsp/

Parent, M., & Reich, B. H. (2012). Governing information technology risk. *California Management Review*, *51*, 134-152. Retrieved from http://cmr.berkeley.edu/

Pezalla, A. E., Pettigrew, J., & Miller-Day, M. (2012). Researching the researcher-as-instrument: an exercise in interviewer self-reflexivity. *Qualitative Research*, *12*(), 165-185. http://dx.doi.org/10.1177/1468794111422107

Pirta, R., & Strazdina, R. (2012). Assessing the need of information technology control environment establishment. *Information Technology & Management Science, 15*(1), 99-104. http://dx.doi.org/10.2478/v10313-012-0014-7

Polit, D. F., & Beck, C. T. (2012). *Nursing research: Generating and assessing evidence for nursing practice*. Philadelphia, P: Lippincott Williams and Wilkins.

Posey, C., Roberts, T. L., Lowry, P., & Hightower, R. T. (2014). Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information & Management*, *51*(5), 551-567. http://dx.doi.org/10.1016/j.im.2014.03.009

Postholm, M. B., & Skrøvset, S. (2013). The researcher is reflecting on her role in action research. *Educational Action Research*, *21*(4), 506-518. http://dx.doi.org/10.1080/09650792.2013.833798

Prindible, M., & Petrick, I. (2015). Learning the building blocks of service innovation from SMEs. *Research Technology Management*, *58*(5), 61-63. http://dx.doi.org/10.5437/08956308X5805008

Rahman, S., & Lackey, R. (2013). E-Commerce systems security for small businesses. *International Journal of Network Security & Its Applications*, *5*(2), 193-210. http://dx.doi.org/10.5121/ijnsa.2013.5215

Raiyn, J. (2014). A survey of cyber attack detection strategies. *International Journal of Security & its Applications*, *8*(1), 247-255. http://dx.doi.org/doi:10.14257/ijsia.2014.8.1.23

Ramanauskaitė, S. S., Olifer, D. D., Goranin, N. N., & Čenys, A. A. (2013). Security ontology for adaptive mapping of security standards. *International Journal of Computers, Communications & Control*, *8*, 878-890. Retrieved from http://journal.univagora.ro/

Razieh, S., & Nasser, M. (2012). An approach to Map COBIT processes to ISO/IEC 27001 information security management controls. *International Journal of Security and Its Applications*. Retrieved from http://www.sersc.org/journals/IJSIA/

Robinson, O. C. (2014). Sampling in interview-based qualitative research: A theoretical and practical guide. *Qualitative Research in Psychology*, *11*(1), 25-41. http://dx.doi.org/10.1080/14780887.2013.801543

Rowley, J. (2012). Conducting research interviews. *Management Research Review*, *35*(3), 260-271. http://dx.doi.org/10.1108/01409171211210154

Rowley, J., Jones, R., Hanna, S., & Vasileiou, M. (2012). Using card-based games to enhance the value of semi-structured interview. *International Journal of Market Research*, *54*(1), 93-110. Retrieved from https://www.mrs.org.uk/ijmr

Rowley, J., Jones, R., Vassiliou, M., & Hanna, S. (2012). Using card-based games to enhance the value of semi-structured interviews. *International Journal of Market Research*, *54*(1), 93-110. http://dx.doi.org/10.2501/IJMR-54-1-093-110

Salazar, A., Soto, R., & Mosqueda, R. (2012). The impact of financial decisions and strategy on small business competitiveness. *Global Journal of Business Research*, *6*(2), 93-103. Retrieved from http://www.theibfr.com/gjbr.htm

Samujh, H. (2011). Micro-businesses need support: Survival precedes sustainability. *Corporate Governance: The International Journal of Effective Board Performance*, *11*(1), 15-28. http://dx.doi.org/10.1108/14720701111108817

Schuesster, J. H. (2013). Contemporary threats and countermeasures. *Journal of Information Privacy & Security*, *9*(2), 3-20. Retrieved from http://jips.cob.tamucc.edu/

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

Shackelford, S. J. (2016). Business and cyber peace: We need you! *Business Horizons*. http://dx.doi.org/10.1016/j.bushor.2016.03.015,

Sheikhpour, R., & Modiri, N. (2012). An approach to map COBIT processes to ISO/IEC 27001 information security management controls. *International Journal of Security & Its Application*, *6*(2), 13-28. Retrieved from http://www.sersc.org/journals/IJSIA/

Singleton, T., & Ursillo Jr., S. J. (2010). Guard against cybertheft. *Journal of Accountancy, 210*(4), 42-49. Retrieved from http://www.journalofaccountancy.com/

Steinmetz, K. K., & Gerber, J. I. (2015). “It doesn’t have to be this way”: Hacker perspectives on privacy. *Social Justice, 41*(3), 29-51. Retrieved from http://www.socialjusticejournal.org/

Stephen, S. K., & Apilado, V. P. (2013). The Sarbanes-Oxley Act, security analyst monitoring activity, and firm value. *Journal of Applied Business & Economics*, *14*(1), 86. Retrieved from Retrieved from www.aebrjournal.org

Symantec. (2016). *Internet Security Threat Report* (21). Retrieved from https://know.elq.symantec.com/e/f2

Teirlinck, P., & Spithoven, A. (2013). Formal R&D management and strategic decision making in small firms in knowledge-intensive business services. *R&D Management*, *43*(1), 37-51. http://dx.doi.org/10.1111/j.1467-9310.2012.00701.x

Theyel, G., & Hofmann, K. (2012). Stakeholder relations and sustainability practices of US small and medium-sized manufacturers. *Management Research Review, 35*, 1110-1133. http://dx.doi.org/10.1108/01409171211281255

Thomas, E., & Magilvy, J. K. (2011). Qualitative rigor or research validity in qualitative research. *Journal for Specialists in Pediatric Nursing*, *16*(2), 151-155. http://dx.doi.org/10.1111/j.1744-6155.2011.00283.x

Thomson, O. P., Petty, N. J., Ramage, C. M., & Moore, A. P. (2011). Qualitative research: Exploring the multiple perspectives of osteopath. *International Journal of Osteopathic Medicine,* 116-124. http://dx.doi.org/10.1016/j.ijosm.2011.06.001

Tsai, J. Y., Raghu, T. S., & Shao, B. M. (2013). Information systems and technology sourcing strategies of e-Retailers for value chain enablement. *Journal of Operations Management*, *31*, 345-362. http://dx.doi.org/10.1016/j.jom.2013.07.009

Urciuoli, L., Mannisto, T., Hinsta, J., & Khan, T. (2013). Supply chain cyber security - potential threats. *Information & Security*, *29*(1), 51-68. http://dx.doi.org/10.11610/isij.2904

Vaismoradi, M., Turunen, H., & Bondas, T. (2013). Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study. *Nursing & Health Sciences*, *15*(3), 398-405. http://dx.doi.org/10.1111/nhs.12048

Verizon. (2016). *2016 Data Breach Investigations Report*. Retrieved from http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

Walker, J. L. (2012). The use of saturation in qualitative research. *Canadian Journal of Cardiovascular Nursing*, *22*(2), 37-46. Retrieved from http://www.cccn.ca

Wang, C., & Wang, S. (2014). User behavior research of information security technology based on TAM. *International Journal of Security & Its Applications*, *8*, 203-209. http://dx.doi.org/10.14257/ijsia.2014.8.2.21

Watts, B. (2011). SEC Says: No new exemptions for small business filers related to Sarbanes-Oxley. *Financial Executive, 27*(5), 15-16. Retrieved from www.financialexecutives.org

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

Yener, S. C., & Cerezci, O. (2016). Material analysis and application for radio frequency electromagnetic wave shielding. *Physica Polonica*, *129*, 635-638. http://dx.doi.org/10.12693/APhysPolA.129.635

Yin, R. K. (2008). *Case Study Research: Design and Methods (Applied Social Research)* (3rd ed.). Thousand Oaks, CA: Sage.

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. http://dx.doi.org/10.1145/2556938

Zamanzadeh, V., Jasemi, M., Valizadeh, L., Keogh, B., & Taleghani, F. (2015). Effective factors in providing holistic care: A qualitative study. *Indian Journal of Palliative Care*, *21*, 214-224. http://dx.doi.org/10.4103/0973-1075.156506

Zhang, H., Zhang, J., Wang, D., & Lu, Y. (2012). Quantitative evaluation of information leakage arising from computer. *International Journal of Applied Electromagnetics & Mechanics*, *40*(2), 101-111. http://dx.doi.org/10.3233/JAE-2012-1432

Zhao, J., & Zhao, S. (2015). Security and vulnerability assessment of social media sites: An exploratory study. *Journal of Education for Business*, *90*, 458-466.

http://dx.doi.org/10.1080/08832323.2015.1095705