2018

Risk Management Strategies to Prevent and Mitigate Emerging Operational Security Threats

Nancy Page Larrimore
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Nancy Page Larrimore

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. Tim Truitt, Committee Chairperson, Doctor of Business Administration Faculty

Dr. Mary Weber, Committee Member, Doctor of Business Administration Faculty

Dr. Z Allen Endres, University Reviewer, Doctor of Business Administration Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2018

Abstract

Risk Management Strategies to Prevent and Mitigate Emerging Operational Security Threats

by

Nancy Page Larrimore

MBA, Webster University, 2013

BS, Coker College, 1999

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

March 2018

Abstract

Dependence on technology brings security compromises that have become a global threat that costs businesses millions of dollars. More than 7.6 million South Carolinians incurred effects from the 162 security breaches reported in 2011–2015. The purpose of this multiple case study was to explore the risk management strategies small business leaders use to prevent and mitigate operational security threats that produce financial losses. The population for this study consisted of 6 business leaders in South Carolina who have demonstrated successful experience in preventing and mitigating operational security threats. Transformational leadership theory provided the conceptual framework for exploring the overreaching research question. Data collection consisted of semistructured interviews with each participant and the collection of company documents that pertained to security procedures, audits, and reviews. Conducting semistructured interviews allowed participants to provide details of real-life experiences. Recorded interviews and transcriptions were analyzed through Moustakas's modified van Kaam method of analysis to identify emerging topics. The 4 themes that emerged were: (a) operational security training and awareness, (b) operational security culture and behavioral effects, (c) operational security policy and compliance, and (d) operational security challenges and risk management. By developing strategies and processes that reflect these themes, small business leaders can reduce financial losses to improve profitability and reduce unemployment, achieving social changes that can benefit society as a whole.

Risk Management Strategies to Prevent and Mitigate Emerging Operational Security Threats

by

Nancy Page Larrimore

MBA, Webster University, 2013

BS, Coker College, 1999

Doctoral Study Submitted in Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

March 2018

Dedication

I dedicate this study to the love of my life and best friend, Tony Walker, for his boundless love and support throughout the doctoral journey. Thank you for never letting me give up, no matter what adversities I encountered. I also dedicate this study to my children, Jaime and Alison, and the three beautiful grandchildren whom they have blessed me with: Hayes, Adiline, and Reese. I would be remiss if I did not include my extended family: Keleigh-Shaye, Thomas, Alexa, Nicholas, Zachary, and our latest blessing, Kasen. This doctoral study is for my beautiful family who has sacrificed much on this journey. Let this milestone in my life serve as a reminder that it does not matter where you come from or where you have been, it is where you are going that matters. With God, all things are possible. My hope is that this achievement will be a source of inspiration to future generations of my family and symbolize that success is a result of discipline, commitment, hard work, and perseverance.

Acknowledgments

I would like to thank God for the grace, strength, and resources to complete this doctoral study. I want to thank my research committee chair Dr. Tim Truitt, for his guidance, mentorship, and counseling throughout this arduous journey. I gave you many reasons to give up on me. I could not have made it, if not for being blessed with you as my chair. Dr. Ron Iden, you have always been ready and willing to help me pull it all together. You provided the needed encouragement, advisement, and edits right down to the last hour. I will be forever grateful. I also wish to thank committee members Dr. Mary Weber, my second committee member, and Dr. Al Endres, university research reviewer (URR) for their guidance and support.

My special acknowledgement is to those who gained their wings before I reached this milestone. My sister Connie, who thought I could do anything. My Joe, who made me *believe* I could do anything. My mother, Ruth, who only wanted my time, something I always had a limited amount of on this journey. There are regrets, and the sacrifices have been numerous and surreal. The last acknowledgment is to my father, H.M., your reverse psychology always worked on me. Don't tell me I *can't*, because I'll show you I *can*. Grace and peace to all!

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

The Internet has become an important means for users to complete business transactions. Information Technology (IT) systems aid in the advancement of business operations, customer service, and stakeholder value (Setia, Venkatesh, & Joglekar, 2013). Business leaders adopt IT innovations within operations to drive efficiencies and increase profitability (Caniëls, Lenarts, & Gelderman, 2015). Although IT services have a positive effect on businesses, IT services introduce data security and privacy issues (Arlitscha & Edelmanb, 2014). Dependence on such technology brings security compromises that have become a global threat and produce financial losses (Feng, Wang, & Li, 2014). Business leaders have serious concerns as they work to respond creatively to new challenges and risks to ensure survival in this highly competitive environment (Patel, Taghavi, Bakhtiyari, & JúNior, 2013).

Background of the Problem

Technology dependence drives a participatory democracy and cultivates organizational innovation, with a concomitant threat of digital piracy (Andersson & Burkart, 2015). The potential knowledge gained through this study could facilitate economic empowerment, expand awareness, and ensure the information security of small businesses (Noor, 2013). New knowledge regarding small business management strategies could lead to improved and effective small business practices (Noor, 2013), which can translate to a higher small business success rate.

The rapid changes in computers and information technology continually initiate new risks to the security of information assets (Patel et al., 2013). Such changes make the

violation of information security easier, and in some cases, undetectable (Lee, Jung, & Lee, 2013). Emerging security threats and impeding breaches increase on average 70% every 3 years, with reported financial losses to U.S. companies of approximately $7.2 million annually (Zafar, Ko, & Osei-bryson, 2015). According to Price Waterhouse Cooper (2013), 93% of large companies and 87% of small businesses in the United States have reported at least one security incident. Small business leaders lack the necessary expertise and often the manpower to combat emerging security threats (White, Hewitt, & Kruck, 2013). Therefore, the objective of my study was to explore successful risk management strategies to prevent and mitigate operational security threats for small businesses in South Carolina.

Problem Statement

Dependence on technology brings security compromises that have become a global threat, costing businesses millions of dollars (Feng, Wang, & Li, 2014). The Federal Bureau of Investigations (2016) reported that 14,032 U.S. companies victimized since October 2013 incurred losses exceeding $3.1 billion. Feng et al. (2014) stated the Computer Security Institute surveyed 738 organizations, reporting an estimated annual loss of $190 million caused by information security breaches. The general business problem is that technology dependence engenders operational security risk, which results in financial losses. The specific business problem is that some small business leaders lack risk management strategies to prevent and mitigate operational security threats, producing financial losses.

Purpose Statement

The purpose of this qualitative multiple case study was to explore the risk management strategies small business leaders use to prevent and mitigate operational security threats that produce financial losses. The population for this case study consisted of six business leaders from four distinct organizations in South Carolina who have demonstrated successful experience in addressing the specific business problem. Positive social change may include a reduction in financial losses for small businesses, improved profitability, and a reduction in unemployment. The social impact of the study results could affect operational security influencing the success of small businesses, which in turn provides jobs and economic growth to communities.

Nature of the Study

The research method for my study was qualitative. A qualitative method of research was appropriate because of the explorative and descriptive nature through which a researcher, using open-ended questions, develops a more expressive view of the business leader through individual experiences, relationships, and norms (Cottrell & Donaldson, 2013). Quantitative studies are a systematic procedure in which numerical data enable examining the relationships and differences among variables (Venkatesh, Brown, & Bala, 2013). Quantitative studies are not appropriate for exploring the strategies to prevent operational security threats. The mixed method approach involves inquiry into various phenomena that cannot be fully understood using only one of the research methods, qualitative or quantitative (Venkatesh et al., 2013). Because I did not

need to examine the relationship among variables resulting from participants' experiences, a mixed method was not appropriate for my study.

The chosen research design was a case study. Using a multiple case study design allows the researcher to develop an understanding of the dynamics present within each organizational setting (Yin, 2013). A multiple case study is particularly relevant to the study of organizations and management (De Massis & Kotler, 2014). I expounded on the development of leaders throughout various situations and over an extended period. Phenomenological researchers interpret human experience from the subjective viewpoint of the participants (Mayoh & Onwuegbuzie, 2013). Because I was not seeking to understand the meaning of experiencing a particular phenomenon, a phenomenological design was not relevant to my study. Ethnography involves shared experiences in cultures or subcultures in specific settings, rather than throughout entire communities (Cruz & Higginbottom, 2013); therefore, ethnography was not applicable to my study. Although I considered alternate qualitative designs, I concluded the case study design best addressed the objective of my study. Therefore, using a multiple case study enabled me to explore multiple facets of the phenomenon while viewing strategies from a variety of lenses.

Research Question

The research question for this study was: What risk management strategies do small business leaders use to prevent and mitigate operational security threats that produce financial losses?

Interview Questions

1. What risks related to the operational security of financial data are associated with your business use of the Internet?
2. Which effective risk management strategies have you implemented to achieve operational security?
3. How do you measure the effectiveness of these strategies?
4. What are some of the challenges you have encountered when responding to operational security threats?
5. How where the challenges to implementing the strategies for risk management addressed?
6. What additional information on developing and implementing strategies to prevent and mitigate security threats can you add that would be valuable to the study?

Conceptual Framework

I used transformational leadership theory as the conceptual framework for this qualitative study. Burns (1978) developed transformational leadership framework and Bass (1985) expounded upon the work of Burns. Together Bass and Burns defined the transformational leadership theory as an attempt by leaders to succeed in raising colleagues, subordinates, followers, clients, or constituencies to a greater awareness of the issues of consequence (Stone, Russell, & Patterson, 2004). According to Kuhnert and Lewis (1987), transformational leadership theory requires leaders with vision, self-confidence, and inner strength to argue successfully for what they see is right or good,

not for what is popular or is acceptable. Transformational leadership is concerned primarily with improving the performance of followers and developing followers to their fullest potential to create future organizational leaders that are both competent and trustworthy (Northouse, 2015). The transformational leadership approach supports and inspires followers, promoting a team-building environment that enhances the attainment of common goals (Northouse, 2015). Transformational leadership initiatives create open communication with individual followers to achieve the organizational goal and to prevent operational security threats (Braun, Peus, Weisweiler, & Frey, 2013). Under the transformational leadership theory, leaders challenge followers to explore new ways to develop and implement management strategies. Transformational leaders seek to transform individual goals into a joint vision for the entire team and develop an innovative approach to emerging operational security threats (Braun et al., 2013). Strategic management theories, leadership, operational controls, and accountability also provided the conceptual framework for my study (Braun et al., 2013). The lens of transformational leadership for reviewing the results of the study could enable a valuable interpretation of the perceptions and experiences of small business leaders.

Operational Definitions

Cloud computing: An on-demand infrastructure hosted on the Internet to store, manage and process data. An on-demand access medium for customers, eliminating the details of service provisioning (Lee, Jung, & Lee, 2013; Moura & Hutchison, 2016).

Cyber security: Processes and practices for protecting networks, computers, programs and data from unauthorized access. Practices for the protection of humans as

potential targets of cyber attacks or even unknowingly participating in cyber attacks comprise an additional dimension (Arlitscha & Edelmanb, 2014; Von Solms & Van Niekerk, 2013).

Information security: Protection, or the measures taken to achieve protection, against unauthorized use of information, especially electronic data. A direct reference to the human factor relates to the role(s) of people in the security process (Sikolia, 2013; Von Solms & Van Niekerk, 2013).

Information security awareness: The general knowledge one has regarding information security threats and the knowledge of specific information security policies related to social engineering threats (AlHogail & Mirza, 2014; Noor, 2013).

Information security behavior: The education of users on security practices during information systems (IS) use that enhances corporate security and reduces security incidents (Montesdioca & Maçada, 2015; Shropshire, Warkentin, & Sharma, 2015).

Information security culture: The collection of perceptions, attitudes, values, assumptions, and knowledge that guide the human interaction with information assets in business for influencing employees' security behavior to preserve information security (Alhogail & Mirza, 2014; Lim, Maynard, Ahmad, & Chang, 2015).

Assumptions, Limitations, and Delimitations

During a study's development, the ability to recognize restrictions and boundaries may occur as designed limitations (Simon & Goes, 2013). My responsibility as a researcher was to provide information and justification for the assumptions, limitations,

and delimitations in my study. In the following subsections, I discuss my study's assumptions, limitations, and delimitations.

Assumptions

Assumptions are facts considered true but that are not verifiable and carry risks to the validity of the study. Assumptions are the hidden perspectives that the researcher assumes to be true, or otherwise, the study may not continue (Merriam, 2014). In the qualitative research method, key assumptions establish how to begin the study (Yin, 2014). My study included small business leaders with successful experience in mitigating operational security threats that produce financial losses. The subjective nature of qualitative research may present questions regarding the validity of the results (Trafimow, 2014). The first assumption in my research was that participants would answer seminstructed and open-ended interview questions honestly. Clearly informing participants of expectations and the confidentiality and ethical responsibilities of the researcher encourages openness in communication (Barker, 2013); the nondisclosure was designed to put participants at ease. The second assumption was that the population of managers in the study would be appropriate for exploring themes involving risk management strategies.

Limitations

Limitations are constraints on the transferability of the findings, which may include biases where participants could confuse the questions and become reluctant to respond, or they are not motivated to do so (Yin, 2014). Awareness of potential bias is imperative to the validity of the study. A researcher must have the ability to set aside any

bias and view the phenomena from a fresh perspective (Yin, 2014). To mitigate bias and presumptions, participants were not colleagues or any individuals with whom I have a personal relationship with in any other manner.

Limitations are also potential weaknesses that could be outside the realm of a researcher's control (Leedy & Ommrod, 2013). One limitation of my study was scheduling interviews at a time that was convenient for participants yet maintaining timely data collection. The second limitation was assuring whether participants understood and answered interview questions honestly. The third potential limitation of the study was knowing if the six semistructured interviews and company documents would provide sufficient information to answer the overarching research question that governed my study.

Delimitations

Delimitations define the boundaries of the study and reflect both conscious exclusion and inclusion of elements during the development of the research plan (Simon and Goes, 2013). Delimitations are components that limit the scope yet include the location, population, and sample size of the study. Unlike limitations, which come from inherent characteristics of method and design and that are beyond the control of the researcher, delimitations result from specific choices by the researcher (Simon & Goes, 2013).

A delimitation for my study was excluding participants with less than one year of employment as a manager in the organizations comprising my multiple case study. I captured detailed descriptions of real-life experiences, as recommended by De Massis

and Kotler (2014), from business leaders on the risk management strategies they have used successfully to prevent or mitigate viable security threats. A second delimitation was the limited geographic location of the organizations comprising my multiple case study. The population of my study consisted of business leaders in South Carolina only. A third delimitation in my study was excluding participants who were not specifically involved with security threat assessment in their companies. Only business leaders involved with operational security threats participated in the study.

Significance of the Study

Every organization is susceptible to the misdeeds of others whether it is internal or external sources, and the threat of a security breach is significant (Feng et al., 2014). The results of this study demonstrate risk management strategies that small business leaders implement to secure organizational information. Findings from the study could promote effective business practices and foster better security understanding. Community relationships could improve through organizational security enhancements protecting businesses and people from new security threats.

Contribution to Business Practice

Organizations and individuals have an increased dependence on technology in the 21st century (Feng et al., 2014). Technological innovations improve lives and streamline business activities, but bring about security compromises that have become a global threat to organizations (Mellado & Rosado, 2012). The number of data breach occurrences continues to climb worldwide and business leaders face increased challenges

managing and monitoring such threats judiciously (Federal Bureau of Investigations, 2015).

Business leaders of large organizations avoid security threats by investing in state-of-the-art hardware and software technology, while small business leaders do not have the same advantages because of limited resources (Galliers & Leidner, 2014; James, 2013). Exploring successful risk management strategies and practices implemented by small business leaders may help to determine effective strategies that other small business leaders can apply (Baur & Schmitz, 2012). Additional results from the study may also equip small business leaders with information to prevent emerging operational threats. The potential knowledge from this study may facilitate economic empowerment, expansion of awareness for small business management, and ensure the information security of small businesses (Noor, 2013). New knowledge regarding small business management strategies from this study could lead to improved and effective small business practices, which translates to higher small business success rates.

Implications for Social Change

Andersson and Burkart (2015) explored the linkages between practices considered transgressive or piratical, their relationship to popular communication, and contribution to social change. The threat of digital piracy forces social change, as technology dependence drives a participatory democracy and cultivates organizational innovation (Andersson & Burkart, 2015). Implementing strategies to prevent security threats may assist business leaders in minimizing the impact on organizational performance and costs to consumers.

A small business affected by security breaches may not overcome the incurred financial losses. The results from this study may contribute new insights into effective strategies that business leaders of small businesses can implement to prevent security breaches (Cant & Wiid, 2013). Small businesses contribute to economic growth through job creation (Majumdar, 2013). Small businesses are typically equal opportunity employers whose workforce includes those in an inadequately represented portion of the workforce (Majumdar, 2013). Successful small business leaders may continue to provide employment for the underrepresented employees who depend upon these jobs for their sustenance (Majumdar, 2013). The implication for social change is the contribution small businesses make to economic growth effecting the potential reduction of unemployment through reductions in small business losses (Coetzee, Preez, & Smale, 2013). Risks associated with information security breaches affect all areas of society (Galliers & Leidner, 2014). Informing business leaders of strategies on effective ways of preventing and mitigating security threats may aid in business growth and profitability for increasing organizations' support for communities (Cant & Wiid, 2013; Coetzee et al., 2013).

A Review of the Professional and Academic Literature

The purpose of this qualitative multiple case study was to identify and explore the successful risk management strategies small business leaders use to prevent operational security threats that produce financial losses. I conducted a literature review to find scholarly and peer-reviewed journal articles, seminal literature, and dissertations to answer the research question and explain the phenomenon of study. My search for peer-reviewed journal articles, as well as books, dissertations, and other research documents

began with using Walden University's library search tools. Information and data from the inquiry contributed to explaining risk management strategies, Internet security threats, identifying gaps in research, and the need for further study.

Human behavior may threaten security deliberately or inadvertently. Information security culture and behavior provided primary consideration by business leaders in workforce development. Information security behavior, improving employee performance, and developing the workforce to its fullest potential are a primary focus in the development of a more potent security solution (AlHogail & Mirza, 2014; Chatterjee, Sarker, & Valacich, 2015; Flores & Ekstedt, 2016; Montesdioca & Maçada, 2015; Northouse, 2015). Information security policy provisions incorporate guidelines for employee reference when interacting with information systems (IS) to business leaders (Da Veiga, 2016). The lack of security of the Internet, and the devices connected to it, results in vulnerabilities (Hill, 2015). Significant increases in Internet threats continue to present an undeniable challenge as Internet dependence continues to increase (Al-Ahmad & Mohammad, 2013; Borrett, Carter, & Wespi, 2014). Business leaders must act promptly and accurately to predict the period and severity of threats they may encounter (Shin, Lee, Kim, & Kim, 2013). Information security awareness among business leaders is emerging through cultural enhancements in perceptions, attitudes, values, assumptions, and knowledge that guide the human interaction when interacting with IS (AlHogail & Mirza, 2014). The implementation of risk management strategies that influence employees' security behavior to preserve organizational information prove positive for information security management (Parra & Hall, 2014). There is a need for business

leaders to consider information security awareness to mitigate risks of Internet security threats in the workplace (Flores & Ekstedt, 2016).

I found 189 journals and other articles for immediate access that I was able to analyze and determine what was appropriate for use in my study. The search engines I used were Thoreau Discovery Service, Business Source Complete, SAGE Research, and EBSCOhost Methods. In the literature review, I provide theories and findings from the exploration of previous researchers regarding operational security threats producing financial losses. Primary search terms were *security breaches, financial losses, information security, information security and culture, information risk strategies*. Secondary search terms included s*ecurity behavior, Internet threats, security failures, employee security and management strategies.* In addition to Walden University's library, I also used Google Scholar for articles, books, and dissertations on information security threats, employee knowledge impact, fraud, behavior, ethics, and values.

Table 1 contains a summary list of peer-reviewed journals, dissertations, books, and nonpeer-reviewed journals referenced in the study. Of the 202 sources noted in Table 1, 186 of the sources had publication dates from 2013 to 2017 comprising 93% of total sources. I used 176 peer-reviewed journal articles that were published no longer than five years ago, equaling 87% of the 202 references. There are 71 total distinct sources with 67 of the articles published less than five years ago. Total and peer-reviewed sources both met doctoral study requirements.

Table 1

Literature Review Source Content

Reference Type	Total	<5 Years	>5 Years	% Total <5 Years
Peer-reviewed journals	189	176	13	93%
Dissertations	2	2	0	100%
Books	8	5	3	63%
Nonpeer-reviewed journals	3	3	0	100%
Totals	202	186	16	92%

The literature review has four main categories: (a) conceptual framework, (b) emerging Internet threat levels, (c) risk management, and (d) management objectives and failures. In the emerging Internet threat levels category, I discuss detection of unexpected threats, the impact on businesses, and the importance of secured Internet communication with absolute data confidentiality, integrity, and availability. The risk management category contains information on security as a major concern for business leaders with rising Internet threats; it also contains information on security culture, user behavior, and the human impact on operational risks while interacting with IS. Management objectives and failures is a category in which I establish strong strategic alignment of attributes between the business and information security at the strategic level. I conclude with a discussion of management objectives and failures.

Conceptual Framework

The focus of my qualitative study was strategies for preventing and mitigating operational security threats. I employed transformational leadership theory to understand computer information security threats affecting the operations of small business in South Carolina. Threats that influence the success of small businesses produce financial losses, affecting jobs and economic growth within communities (Noor, 2013). I explored risk management strategies that may improve information security cultures, which affect employee behavior when exposed to vital information.

Burns (1978) developed a transformational leadership framework that Bass (1985) expanded on. Bass and Burns defined transformational leadership theory as an attempt by leaders to succeed in raising colleague, subordinate, follower, client, or constituency awarenesses of consequences (Stone et al., 2004). In the 21st century, we have become increasingly dependent upon technology, relying on the Internet for business. While Internet dependence continues to grow, so does the risk of the invasion of personal and financial information (Al-Ahmad & Mohammad, 2013). Business leaders must focus on information security behavior, improving the performance of their followers, and developing the workforce to its fullest potential (Northouse, 2015). Transformational leadership supports and inspires followers in the information security culture and promotes a team-building environment for enhancing the attainment of common goals (Northouse, 2015).

According to Parra and Hall (2014), information security culture is a collection of perceptions, attitudes, values, assumptions, and knowledge. Information security culture

can guide human interaction with in an organization to influence employee security behavior preserving security information (AlHogail & Mirza, 2014; Parra & Hall, 2014). I sought to identify and explore strategies for improving such cultures. Kuhnert and Lewis (1987) referred to transformational leadership as a theory that requires leaders with vision, self-confidence, and inner strength to argue successfully for what they see is right or good, not for what is popular or acceptable. In conjunction, the theory of planned behavior I used to argue that factors such as experience and knowledge can influence behavior indirectly by influencing behavioral, normative, and control beliefs. The effects of planned behavior produce a positive cultural effect in the domain of compliance involving information security policy (Flores & Ekstedt, 2016; Sikolia, 2013). In the changing world of technology, business leaders must have vision and the strength to uphold the moral values of the organization (Kuhnert & Lewis, 1987); reducing financial losses for small businesses can improve profitability and reduce unemployment to effect beneficial social changes (Noor, 2013). Planned transformational leadership heightens the role of information security awareness that influences social security behavior (Flores & Ekstedt, 2016). Therefore, operational security influences the success of small businesses, which in turn provides jobs and economic growth.

Transformational leadership initiatives create open communication with individual followers to achieve organizational goals and to prevent operational security threats (Braun et al., 2013). Under the transformational leadership theory, business leaders can challenge employees to explore new ways to develop and implement risk management strategies preventing security breaches. Transformational leaders seek to

change individual goals into a joint vision for the entire team and develop an innovative approach to emerging operational security threats (Braun et al., 2013). Using the lens of transformational leadership for reviewing the results of this study could facilitate interpretation of the perceptions and experiences of small business leaders to enhance information security.

Emerging Internet Threats

One of the major challenges faced by businesses is the response time to Internet threats. According to Shin et al. (2013), business leaders must act promptly while accurately predicting the period and severity of threats. The Internet takes on a network capability that is a vital part of current business transactions. The Internet has become an essential and indispensable means for users to complete relevant business. The network economy is born based on commerce. Referred to as e-commerce, such Internet activity has expanded both foreign and domestic businesses. Wu and Shan (2015) indicated that the current network security economy is not optimistic. Networks and IS have inherent disadvantages such as the vulnerability to threats they present. These disadvantages make network security an important part of the country and national defense security and are a critical bottleneck, restricting the further development of the network economy (Dunn, 2013; Kello, 2013; Networking and Information Technology Research and Development [NITRD], 2016; Wu & Shan, 2015). The influence of the Internet enhances the popularity of computer network systems. Network security becomes more critical as security threats arise.

Chen, Zuo, Huang, and Guo (2016) described security techniques, such as user authentication, data encryption, and firewalls, that use improved security networks; however, there are still many unsolved security problems. With limits placed on standard security techniques, researchers began to focus on building systems called intrusion detection systems (IDS). Detection of unexpected and emerging new threats have become a necessity for secured Internet communication with absolute data confidentiality, integrity, and availability (Aneetha & Bose, 2014). To detect Internet attacks in advance, the importance of intrusion forecasting in a network intrusion system is growing rapidly (Shin et al., 2013). Shin et al. (2013) proposed approaching intrusions with existing detection systems might assist in leading to earlier discovery of attacks. Prior research demonstrates that an ensemble of several different techniques performs better than each technique individually (Chen et al., 2016; Shin et al., 2013). Advanced detection approaches from combining or integrating multiple learning techniques have shown better detection performance than general single learning techniques (Lin, Ke, & Tsai, 2015; Shin et al., 2013). Implementation of such detection systems proved to be not only accurate and fast, but also helpful for increasing effectiveness of the surrounding network (Aneetha & Bose, 2014).

As technology continues to evolve rapidly, new security risks and challenges arise. Lee, Jung, and Lee (2013) indicated new obstacles can arise from cloud computing. Cloud services are collections of a variety of technologies and services and have the characteristics such as resource efficiency through virtualization and energy efficiency and reusability. Lee et al. reported increases in cloud service markets at an expected

annual growth rate of 18.9% exceeding 1,768 billion. Companies and individuals are expanding consideration of cloud computing technology through marketing as a cost-effective method for small businesses to innovate (Gupta, Seetharaman, & Raj, 2013). The concern regarding this shared environment directs attention to standards, regulations, and the capability consistent with technological evolution (Lee et al., 2013). Bendovschi and Ionescu (2015) analyzed the gap between the rapid technological evolution and the supporting standards and legislation regarding assurance, reliance, and information security. The distributed and open structure of cloud computing services becomes an attractive target for potential cyber attacks by intruders (Patel et al., 2013). Increased intrusion exists in part because IDS are largely inefficient for deployment in traditional cloud computing settings, as open structures in shared environments make it a lucrative target for cyber attacks (Patel et al., 2013).

Increased technology dependence. Pawlik (2014) posited that the formation of the Internet based its foundation on openness and freedom, which has spiraled into an incredible tool for connecting people around the world. The Internet's openness and freedom has changed the lives of many both positively and negatively. The Internet has become a resource for the billions of people who now rely on it in their daily lives. There are many concerns, the most significant being information security and privacy. According to Pawlik, such issues remain a point of focus, debated since the Internet's inception. The cyber security situation is worse than most people imagine (Hill, 2015). An accelerating pace of technological change causes the future to be more difficult to predict with each passing year (Borrett et al., 2014). The lack of security of the Internet

and the devices connected to it results in serious vulnerabilities (Hill, 2015). Undeniable challenges exist, as Internet dependence continues to increase (Borrett et al., 2014; Pawlik, 2014).

Concern about the security of computing systems has existed for over 40 years and that concern has intensified with the widespread global interconnectedness enabled by the Internet (Hill, 2015; NITRD, 2016). In the last 20 years, the proliferation of the Internet brought about e-commerce, which lends itself to the coining of the term *network economy* (NITRD, 2016). The Internet enters the market as an essential tool for many businesses both foreign and domestic. Given the world's dependence on the network economy, the lack of inherent security present in network and IS makes for less than ideal market conditions for business (Al-Ahmad & Mohammad, 2013). The result is a need for security at both a local and national level to mitigate risks. While security is a major issue, at the same time, the need to remove barriers to the growth brought about by the network economy is relevant (Kello, 2013). To accomplish these simultaneous needs, Wu and Shan (2015) reported on a method to enhance network and information security prevention in a timely and effective manner referred to as *data mining*. Technology from web data mining provides the blending of both historical and new data technologies to increase security while propelling necessary market growth. Wu and Shan indicated web data mining is an advanced technology that offers the possibility and feasibility of enhanced performance of network information security.

According to Lagazio, Sherif, and Cushman (2014), human dependency on digital communication and other networked technologies for tasks ranging from simple web

browsing to monetary transactions has continued to increase since the inception of the Internet. Technology is now prevalent in modern society, transforming people's everyday lives and work environments (Hynes, 2013). Internet dependency has rendered a growing intensity on the strategic relevance of cyberspace; therefore, enabling the achievement of elemental objectives in present day societies that includes innovation, collaboration, productivity, competitiveness, and leadership (Hynes, 2013; Lagazio et al., 2014). With the expansion of such objectives, online criminal activity can take place.

Rising security breaches. Cyber security often is synonymous with the term information security are not exact equivalents (Von Solms & Van Niekerk, 2013). Cyber security expands beyond the limits of information security to encompass other assets beyond information resources to include people as possible targets of cyber attacks (Von Solms & Van Niekerk, 2013). Additionally, cyber security includes people as unwitting participants in cyber attacks. Typically, information security only considers the human factor as it relates to their roles in the security process. This additional measurement has moral ramifications for society in general since the assurance of certain susceptible groups could take shape as a societal responsibility (Von Solms & Van Niekerk, 2013). Criminal activities and security breaches often referred to as attacks do not only represent technological threats. Economically developed societies are increasingly becoming information societies which are followed by rising security threats to information that negatively impact the core of these societies (Kello, 2013; Lagazio et al., 2014). Although no one disputes the importance of protecting cyberspace from criminal activities, our understanding of cybercrime and its consequences, both economic and

social, is still limited. The literature on cybercrime is vast but still theoretically thin and underdeveloped. Undeveloped literature exists because there are still many different perspectives on the topic, leading to a lack of consensus regarding many fundamental aspects of cybercrime (Lagazio et al., 2014).

As the Internet becomes the essential tool for businesses, continued growth in e-commerce becomes a leader in the network economy. The expansion of cyber functionalities opens new opportunities for people to carry out online criminal activities (Lagazio et al., 2014). Unethical use of the Internet has led to serious security concerns (Chatterjee et al., 2015). The use of point of sale for business transactions becomes the primary information source for retailers, and the United States may undergo a drastic increase in information security threats through e-commerce fraud (National Institute of Standards and Technology [NIST], 2016). The advantages of the Internet come with risks, as people use the innovative tool as a medium for criminal objectives (Lagazio et al., 2014). Security risks of e-commerce transactions influence consumers, retailers, payment processors, banks, and card issuers. Retailers bear the cost for fraudulent, card-not-present (CNP) transactions, motivating them to reduce fraud in order to avoid damage to their reputation which impact revenue (Hills & Anjali, 2017; Von Solms & Van Niekerk, 2013).

Criminal activities often referred to as *attacks*, do not only represent technological threats but creates issues with individuals also. Acceptance of modern economically developed societies continues to increase, transforming them into information societies. Security attacks on privacy and information threatens the core of these societies (Dunn,

2013; Eriksson & Giacomello, 2006; Lagazio et al., 2014). Although no one disputes the importance of protecting cyberspace from criminal activities, our understanding of cybercrime and its consequences, both economic and social, remains limited. The literature on cybercrime is vastly underdeveloped because currently there are many different perspectives on the fundamental aspects of cybercrime (Lagazio et al., 2014).

Increased financial losses. Cyber security attacks can disrupt the normal operation of computing systems by denying service to the user (NITRD, 2016). These attacks may damage systems with computing components, by altering the computer control of physical devices, causing the theft of proprietary, secret or private information (NITRD, 2016). The National Cybersecurity Center of Excellence (NCCoE) monitors and reports on the topic of multifactor authentication for e-commerce. Implementing greater security control mechanisms at the point of sale encourages a forceful increase in electronic commerce fraud to retailers in the United States (NIST, 2016). The security risks of e-commerce transactions affect all consumers, retailers, payment processors, banks, and card issuers (NIST, 2016). Retailers bear the cost for fraudulent transactions, motivating them to reduce fraud in order to avoid damage to their reputation and market position (Järveläinen, 2013). Any organization is susceptible to a breach of security from outside such as hacking, product contamination and theft of intellectual property (NIST, 2016). These are all risks to any size business and can be extremely detrimental to financial health and reputation, and threats posed by a malicious insider can be even more challenging (Hills & Anjali, 2017). The financial impact of fraudulent activities

motivates business leaders to pursue security solutions to eliminate potential revenue losses. Losses in revenue estimate to be over $3 billion dollars (NIST, 2016).

With the development of cyber functionalities, come new opportunities for online criminal activities. Hacker groups, criminal organizations, and espionage units have worldwide access to powerful, evolving capabilities, which they use to identify, target, and attack their victims (Lagazio et al., 2014). These attacks are not symbolic of technological threats but include societies as a whole. Through the acceptance of such cyber functionalities, we accept that modern, economically developed societies as information societies. Threats to information, based on the acceptance, might also pose risks to the core of the societies we embody (Eriksson & Giacomello, 2006; Lagazio et al., 2014). Although no one disputes the importance of protecting cyberspace from criminal activities, our understanding of cybercrime and its consequences, both economic and social, is limited. The literature on cybercrime is vast, but still theoretically thin and underdeveloped. With many different perspectives on cybercrime, there remains a divided consensus on the fundamental aspects which leaves much literature undeveloped (Lagazio et al., 2014).

Risk Management

Information security is a major concern of risk management for business leaders. Due to the frequency of changes in computer environments, and information technology in general, new risks are always inherent to information security assets (Nazareth & Choi, 2015). These risks potentially make it easier to compromise the security of information assets and such compromises may even go unnoticed. Security solutions based on the

technical aspect alone are not sufficient to protect operational information of businesses (Montesdioca & Maçada, 2015). Organizations must develop their capabilities to respond to and mitigate risks. Developed capabilities are a strategic strength in highly competitive areas, as well as essential to the longevity of the organization. While organizations have developed, implemented, and enhanced security controls over time, the current information security controls and practices may not be sufficient to protect organizations because security must take into account people as a potential threat, in addition to technical security (AlHogail, 2015). As businesses provide employees with access to IS and the frequency and sophistication of security threats grows, the need to provide security assumes greater importance (Nazareth & Choi, 2015). Successful information security is dependent on the behavior of the employee, or user, while operating the IS. User satisfaction is widely used to measure the success of IS (Montesdioca & Maçada, 2015).

Studies by Montesdioca and Maçada (2015) indicated that the achievement of a strong information security presents itself through a combination of technical and socio-organizational investments that considers the user as an active agent. User satisfaction is one of the most relevant variables to assess the success of IS. The user satisfaction variable in conjunction with the information system is important because it suggests business leaders are investing in the decision-making process of the user (Barton, Tejay, Lane, & Terrell, 2016; Montesdioca & Maçada, 2015; Zia, 2015).

Information security culture. Information influencing employees' security behavior to preserve information security within an organization security culture defined

as the collection of perceptions, attitudes, values, assumptions, and knowledge that guide the human interaction with information assets (AlHogail & Mirza, 2014; Parra & Hall, 2014). The achievement of successful information security may occur through a combination of technical and socio-organizational investments that consider the user as an active agent (Montesdioca & Maçada, 2015). AlHogail and Mirza (2014) expounded on information security culture supporting technical security methods to make information security a natural part of employees daily work activities. Information security culture involves identifying the security-related ideas, beliefs, and values of the business group. Such identification shapes and guides security-related behaviors of employees of the business. Previous researchers have debated the extent to which security culture might potentially affect the security of the organization. Prior research presented the argument on how employee interaction with the organization's systems and procedures at any point in time could affect results (AlHogail & Mirza, 2014). Montesdioca and Maçada (2015) contended that the success of information security depends on appropriate user behavior while interacting with IS.

Current and former employees are a root cause of information security incidents (Da Veiga & Martins, 2015). Establishing information security cultures in organizations affects employee perceptions and security behavior in a way that can guard against information security threats posed by insiders (AlHogail & Mirza, 2014). One way of addressing the human aspect is to embed an information security culture where the interaction of employees with information assets contributes to the protection of these assets (Da Veiga & Martins, 2015). The development of a comprehensive information

security culture framework for organizations is a concern for business leaders. AlHogail and Mirza (2014) introduced the structured strategy, technology, organization, people, and environment (STOPE) scope. STOPE, a base for a cultural framework, is a guideline for various issues of information security to integrate. AlHogail and Mirza's human factor concept framework incorporates four main domains that influence information security behavior: preparedness, responsibility, management, and society and regulations.

To improve user security behavior, AlHogail and Mirza's (2014) suggested that the information security culture carefully consider human factor domains below:

1. The *preparedness domain* is mainly concerned with training and awareness, knowledge acquisition, and change of old practices.
2. The *responsibility domain* is mainly related to employees' practices and performance such as monitoring and control, reward and deterrence, and acceptance of responsibility.
3. The *management domain* is concerned with security policy, practice, direction, and interaction issues.
4. The *society and regulations domain* relates to social and cultural aspects and regulation issues (p. 4).

The illustration shown in Figure 1 represents the human factor framework.

Figure 1. The human factor framework. Adapted from "Design and Validation of Information Security Culture Framework," by A. AlHogail, 2015, *Computers in Human Behavior*, *49*, p. 569. Copyright 2015 by Elsevier Ltd.

The human factor framework incorporates change management principles that guide the cultivation of the information security culture (AlHogail & Mirza, 2014). Validation of feedback on the correctness and comprehensiveness of the framework structure and its associated tasks materialize by surveying experts in the field. Additionally, research provided by the cultural framework might aid businesses in the development of an effective information security culture protecting their information assets. Da Veiga and Martins (2015) argued that it is critical to improving the information security culture in organizations, such that the behavior of employees complies with information security, and related information processing policies and regulatory requirements.

Assessment of information security cultures takes place by using an approach such as an information security culture assessment (ISCA). The empirical data derived from an ISCA might influence the information security culture by focusing on developmental areas, of which awareness and training programs are a critical facet (Da Veiga & Martins, 2015; Line & Albrechtsen, 2016). Research provided by Da Veiga and Martins (2015) illustrated that the theoretical ISCA tool previously developed may include implementation in organizations to influence the information security culture in a positive manner. Empirical evidence occurred indicating that information security training, and awareness is a significant factor in positively influencing an information security culture when applied in the context of ISCA (Da Veiga & Martins, 2015). The objective of ISCA is to help organizations foster an information security culture. In this cultured environment the nature, confidentiality, and sensitivity of information takes place, and employees handle information accordingly. ISCA aids in identifying components an organization might use to protect the organization's information from a human perspective (Da Veiga & Martins, 2015).

Information security behavior. The success of information security depends on appropriate user behavior, while interacting with IS (Line & Albrechtsen, 2016; Montesdeoca & Maçada, 2015). Organizational leaders must take action to investigate the cognitive factors that influence behavior. Understanding behavior is important in designing an effective information security policy. Montesdioca and Maçada (2015) found user satisfaction evaluated the cognitive aspects of the utilization of IS. User

satisfaction might provide the data required to align information security policies with user information system requirements (Da Veiga, 2016; Montesdioca & Maçada, 2015).

Flores and Ekstedt (2016) defined information security awareness as an employee's general knowledge about information security threats and their knowledge of specific information security policies related to operational security threats. Flores and Eksedt further found that information security awareness shaped an employee's own interest and experiences, or through interventions carried out by the organization's information security management group. The role of information security awareness influences the behavior presented in actions taken in information security (Kearney & Kruger, 2016). Shared organizational culture may influence individual employee beliefs, and therefore, form a given behavior. Organizational culture influences information security behavior and significantly effects the measure of accountability, confidentiality, and availability of employees (Gu, Hoffman, Cao, & Schniederjans, 2014; Järveläinen, 2013). An environment that information security culture correlates directly with is the employee's information security awareness, attitude, and beliefs regarding information security threats (Flores & Ekstedt, 2016; Pfleeger, Sasse, & Furnham, 2014).

Flores and Ekstedt (2016) suggested that an employee might be aware of information security related threats based on past experience or interests. The employee can also have knowledge about specific policies, which might require him or her to undergo specific training on policies (Da Veiga, 2016). Da Veiga (2016) further noted additional training makes an employee aware of acceptable uses of IT products and services, as outlined in an organization's policy. The policy governs the management of

sensitive and confidential information. Employee information security awareness shapes their own interest and experiences or by interventions carried out by the organization's information security management group (Da Veiga, 2016; Flores & Ekstedt, 2016). Sikolia (2013) indicated that experience and knowledge could influence behavior indirectly by normative and controlled beliefs. Tested and identified experience and knowledge can have a positive effect in the understanding of information security policy compliance. Cyber security neglect may occur in the early stages of design of new domains and computing use (NITRD, 2016). Human behavior may threaten the security of the behavioral computing system, deliberately or inadvertently (Chatterjee et al., 2015; Montesdioca & Maçada, 2015). Consideration of human behavior by business leaders, as part of a more potent cyber security solution, is vital (Chatterjee et al., 2015; Gu et al., 2014; Montesdioca & Maçada, 2015; NITRD, 2016; Sikolia, 2013).

The adoption of computer and Internet technology is better in the way businesses operate (Line & Albrechtsen, 2016). The risk to the confidentiality, integrity, and availability of organizational data and systems has seen improvement as well. Information security is an ever-present concern for all organizations (Chatterjee et al., 2015). Financial estimates of the impact of security breaches to information and technology resources range from hundreds of billions to over one trillion dollars each year worldwide (Sikolia, 2013). Organizations continue to develop a combination of technical, administrative, and physical controls to reduce information security risk. Administrative measures include the development of information security policies (Sikolia, 2013). The development of policies included outlines of the duties and

responsibilities of the employee to safeguard the information technology resources of their organizations (Montesdioca & Maçada, 2015; Sikolia, 2013).

Chatterjee et al. (2015) reported that most security violations are a result of insiders using IT in an inappropriate manner. Employees using IT inappropriately present a significant security threat to businesses (Chatterjee et al., 2015). Information security policy provisions incorporate guidelines for employee reference, when interacting with IS to secure the data and technology resources of their employer (Da Veiga, 2016). Regrettably, there are documented cases of employee intentional and nonintentional noncompliance with information security policies (Chatterjee et al., 2015). Security experts concluded through documented cases that employees are the weakest link in information security defenses (Chatterjee et al., 2015). Evidence suggests that a preponderance of information security incidents occur driven by trusted employees' actions (Crossler et al., 2013; Sikolia, 2013). However, popular media tends to headline the exploits of hackers or crackers (Crossler et al., 2013; Sikolia, 2013).

Information security management. It is imperative that business leaders recognize the importance of creating a compatible culture, which ensures security. Greater participation by business leaders in ascertaining information security leads to greater assimilations in operations of the business (Barton et al., 2016). Good information security management is a function of effective communication structures. The need for establishing communication structures may seem elementary, but the relevance of ensuring adequate information security is paramount (Lim, Maynard, Ahmad, & Chang 2015). The protection of information resources from a comprehensive range of security

threats must be a primary objective for business leaders. Businesses of all sizes must implement information security management (ISM) practices, which apply a broad spectrum of managerial and technical controls, in pursuit of information security objectives (Lim et al., 2015).

According to Dhillon, Syed, and Pedron (2016), continuous improvement may not occur; therefore, the integration of cultural processes for a sustained cultural integration is imperative. Failure to do so may cause dissatisfaction, resulting in disgruntled employees that neglect their integrative efforts collimating a serious security concern. Dhillon et al. depicts that change is a complex and a circular process, and there is a need to continuously evaluate and reevaluate how formal changes affect informally and subsequently institutionalized. Typically, organizations stop the change management process now. The majority of security breaches, however, occur during the post-implementation stage of the technical edifice. As illustrated in Figure 2, a redefined set of formal structures follows technical implementation and many failures become obvious at this point (Dhillon, et al., 2016; Goo, Yim, & Kim, 2014).

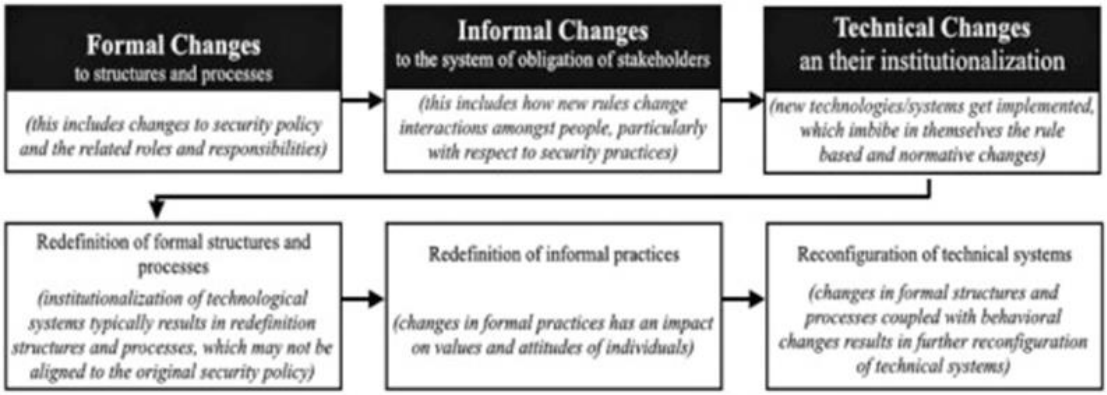


Figure 2. Operational changes: formal, informal, and technical. Adapted from "Interpreting Information Security Culture: An Organizational Transformation Case Study," by G. Dhillon, R. Syed and C. Pedron, 2016, *Computers & Security*, *56*, p. 68. Copyright 2015 by Elsevier Ltd.

Increasing demands for security risk assessments for network and IS usually arise when a variety of internal or external threats exist. With the increasing complex scale of network and IS, information system security risks may be more difficult to assess (Ye, Wandong, & Nan, 2016). Organizations spend over $70 billion on IT security but are unable to protect the organization, since cyber criminals routinely discover exploits and breach defenses (Soluade & Opara, 2014). Human made or natural threats apply in existing vulnerabilities of network and IS that incur security incidents. Implications on the mechanism for the information assets damaged in incidents apply. Information security risk evaluation comprehensively evaluates the information system and information security properties that include confidentiality, integrity, availability, controllability, and undeniability. All properties, that when in storage, process or transmit based on the scientific and fair methods of information security safeguard technology.

The purpose of controlling secure risks, in a certain range, is achieving a secure operation of an information system (Ye et al., 2016). IS secure risk evaluation helps to obtain the secure state of the system and its environment. Risk evaluations help clear the responsibility at all levels during system construction. Also, risk evaluations can enhance a more effective and secure assurance measures (Ye et al., 2016).

Management Objectives and Failures

ISCA information security provided by Da Veiga and Martins (2015) is to help organizations foster an information security culture aiding business leaders in forming strategies to preclude failures. Employees must understand management's objective in promoting information security culture. Business leaders may highlight specific focus areas for the business and focus on enabling the workforce to align themselves with the businesses information security requirements (Da Veiga & Martins, 2015).

Frequently, the cost arising from a data breach is not imminent, and containing costs require proactive action. Prompt and efficient handling of a data breach is imperative to containing costs (Caldwell, 2014). In order to act proactively, business leaders must prepare for what some believe to be the inevitability of data breaches. Caldwell (2014) revealed that the growing awareness of the potential impact of a data breach would inevitably spur some businesses leaders into action. There is a real risk that some business leaders may take the opposite approach. Such accessions by business leaders are hackers are too good to stop and exacerbates risks. Therefore, a lack of investment to prevent security threats, hacking, may exorbitantly exist. Presenting a

passive approach to security can be extremely dangerous and detrimental to the success and profitability of a business (Caldwell, 2014).

Workforce development. Dhillon et al. (2016) assessed previous arguments made that change in a complex circular process. The circular process proceeds from formal to informal, to technical, to new formal, with the emphasis shifting rather rapidly at certain junctures. To understand the nature of these intra-relationships, it is important to understand the dynamics of change, which in turn can lead to a better understanding of the transformation process (Dhillon et al., 2016). The enhanced understanding can help analyze business processes that affect the state of current and future information security (Dhillon et al., 2016; Goo et al., 2014). Security aspects are different for each organization. ISCA aids management in determining where business leaders might focus security efforts (Da Veiga & Martins, 2015). ISCA helps the business to optimize money, resources, and time spent on cultivating an acceptable information security culture. Employees that receive information security training presented a more positive information security culture than those who did not undergo such training (Da Veiga & Martins, 2015).

The level of an organization's information security culture might improve through the implementation of recommendations (Da Veiga & Martins, 2015). The application of ISCA in a range of contexts contributes to the relevance and effectiveness of the ISCA tool. The value derivative of focusing attention to the developmental areas identified by ISCA through the implementation of specific action plans proves decisive. Attending to information security training and awareness has a positive impact on the information

security culture and enhances the culture over time (Line & Albrechtsen, 2016). As a positive influence on the information security culture, the human element and employee behavior gives direction through the implementations of corrective actions (Da Veiga & Martins, 2015).

Business leaders now see the importance of workforce development regarding security (Caldwell, 2014). Researchers continue to expound on a more cost-effective way of preventing security threats by investing more money in people (Da Veiga & Martins, 2015). A more proactive approach to improve information security by businesses of all sizes is imperative. According to Caldwell (2014), businesses must assess operational data and consider which data is critical, what the value of that data is and who might want it. For businesses to be prepared for security attacks and avoid costly data breaches, leaders must understand the methods and techniques that cyber criminal utilize to infiltrate the operating systems (Caldwell, 2014). The importance of user education to improve information security is significant. A preponderance of security breaches minimizes through improved education of employee and users. However, the investment made in educating employees typically represents less than one percent of the overall security budget (Caldwell, 2014). Focusing on information security training and awareness has a positive influence on the information security culture and enhances the information security culture over time. The human element has a positive influence on the information security culture. Influence directly relate to corrective actions toward employee behavior (Da Veiga & Martins, 2015).

Yaokumah and Brown (2014) disclosed that the realization of value information security investments occur when strategic organizations increases the chance of selecting information security investments: (a) with the highest potential of creating business value, (b) by increasing the likelihood of successful execution of selected investments, and (c) by reducing the risk of failure, particularly those risks that have high impact on the organization. Business leaders must evaluate information security investments to ensure increased business value. Value achievement can take place through a reduction of unnecessary costs, improved quantity and quality of services, and enhanced overall level of confidence among the stakeholders (Yaokumah & Brown, 2014). Productive value delivery occurs on security investments of the business through proper management.

Governance. Da Veiga and Martins (2015) placed importance on information security, from the International Standards Organization (ISO), for risk and compliance officers, and information security managers. ISCA can aid management in directing and prioritizing information security awareness and training because ISCA highlights the topics and biographical groups in the organization that require attention. ISCA provides insight into possible approaches that organizations can adopt to reduce the risk to the protection of information from an employee perspective (Da Veiga & Martins, 2015). Von Solms and Von Solms (2004) published the 10 Deadly Sins of information Security Management. The points, if not taken into account while developing a governance plan, could cause the plan to fail, or at the least, cause serious flaws in the plan. Von Solms and Von Solms suggested that management use the 10 points as a checklist to ensure the introduction of a comprehensive plan is defined.

The 10 Deadly Sins of Information Security Management introduced by Von Solms and Von Solms (2004) are:

1. Not realizing that information security is a corporate governance responsibility (the buck stops right at the top).
2. Not realizing that information security is a business issue and not a technical issue.
3. Not realizing the fact that information security governance is a multi-dimensional discipline (information security governance is a complex issue, and there is no silver bullet or single 'off the shelf' solution.
4. Not realizing that identified risks are the foundation for an information security plan.
5. Not realizing (and leveraging) the important role of international best practices for information security management.
6. Not realizing that a corporate information security policy is absolutely essential.
7. Not realizing that information security compliance enforcement and monitoring is absolutely essential.
8. Not realizing that a proper information security governance structure (organization) is absolutely essential.
9. Not realizing the core importance of information security awareness amongst users.

10. Not empowering information security managers with the infrastructure, tools, and supporting mechanisms to properly perform their responsibilities (p. 2).

Addressing all 10 issues could be useful for implementing or evaluating an existing information security plan in a company that seems to be having problems in being effective. Von Solms and Von Solms (2004) revealed that ignoring even one of these facets, or not properly taking each into account, serious problems in introducing and maintaining a proper information security plan in a company might arise. Neglecting any point might result in companies experiencing severe problems in implementing a successful comprehensive information security plan within the company (Von Solms & Von Solms, 2004).

Enron and WorldCom experienced business collapses (Al-Zwyalif, 2013). In response to scandals brought about by the collapse of these businesses, the U. S. Congress passed the Sarbanes-Oxley Act (SOX) in 2002 (Karanja & Zaveri, 2014). The SOX Act is most widely known as the enhancement of information reported in the financial statements. The SOX Act's primary purpose is to provide protection to investors and other stakeholders, strengthen the internal controls, and prevent financial statement fraud (Al-Zwyalif, 2013; Spears, Barki, & Barton, 2013). However, the realization of the need for IT governance also increased considerably during the collapse of Enron and WorldCom **(**Karanja & Zaveri, 2014). Therefore, several sections of the SOX Act directly affected the IT governance, establishing an integral part of overall enterprise governance. Because of the significant role that technology plays in the security and stability of accounting information systems (AIS), IT governance is a vital part of the

SOX Act. SOX requires an external audit of AIS and IT processes that significantly affect corporate financial reporting (Spears et al., 2013). Chen (2016) stated that the financial statement is the main basis for decision-making on the part of a vast number of business leaders, as well as a concrete expression of business performance. A primary goal of SOX provides information security to accounting information provided to financial statement users (Al-Zwyalif, 2013).

Al-Zwyalif (2013) measured the direct effects of IT governance on the usefulness of accounting information provided by the financial statements. Investigations into the indirect effect of IT governance on the usefulness of technology and its efficiency directly affected AIS results. Al-Zwyalif's research sheds light on the role IT governance plays in securing vital information while improving the usefulness of information provided through technology enhancements. Karanja and Zaveri (2014) provided insight into relationships among IT governance, AIS, and the usefulness and efficiency of accounting information reported in the financial statements.

According to Williams, Hardy, and Holgate (2013), achieving a sustainable information protection capability within a complex business, legal, and technical environments is an integral part of supporting an organization's strategic and compliance objectives. Flores, Antonsen, and Ekstedt (2014) presented an empirical investigation on what behavioral information security governance factors drive the establishment of information security knowledge sharing in organizations. Information security can complement IT Governance (ITG) in the assurance of the confidentiality, integrity, and availability of information (Fazlida & Said, 2015; Nykänen & Kärkkäinen, 2016; Spears

et al., 2013). The growing emergence of information security threats call for information security to be integrated into the organization's corporate governance, and treated as high importance, as other critical corporate governance area by executive management. While senior level management have leading roles, the findings point to other significant actors such as outsourcing partners and lower level management (Williams, 2013; Williams et al., 2013). A concept to enforce information security derived from corporate accountability and information governance attempts to make corporate level executives aware of their responsibility in the protection of data. Information security is an integral feature of information governance (Williams et al., 2013). Business leaders at the strategic level establish strong alignment between the business and information security with the aim of ensuring that security delivers business value through appropriate policies of risk management, resource management, and performance measurement (Williams et al., 2013). Business leaders must improve strategic alignment attributes in order to attain effective information security governance.

Yaokumah and Brown (2014)'s study strongly supported the foundational understanding of information security governance and the effectiveness governance based on: (a) the commitment of the organization's stakeholders with the purpose of aligning key stakeholder's interest with business objectives, (b) availability of resources with the aim of strategically manage resources and competencies to achieve organizational goals, and (c) the responsibility and accountability of the agents to ensure that performance through monitoring and measurement is efficient and effectively monitored in order to minimize risks.

Audit and compliance. Employee negligence or ignorance of information security policies are the cause of many of the recent security breaches reported (Sohrabi, Von Solms, & Furnell, 2016). Such negligence results from significant financial losses for businesses. Previous studies have rendered insights into the instrumental view of employee compliance and the importance of behavioral issues (Goo et al., 2014). Business leaders strive to implement influential policies and procedures to improve information security. The impact of policies and procedures bare close examination as compliance with information security continues to be problematic for business leaders (Goo et al., 2014; Sohrabi et al., 2016). Jahyum et al.'s (2014) behavioral model, integrated the role of top management and organizational culture into planned information security behavior to understand how business leaders, might influence the security compliance behavior of employees.

The Internet and information technology continue to have an enormous influence on human life (Haigh, Russell, & Dutton, 2015). Information security continues to be a decisive concern for both users and organizations. Technology cannot solely guarantee a secure environment for information. In addition to technology, the human factor of information security must be considered. The lack of information security awareness, ignorance, negligence, apathy, mischief, and resistance are the root of user mistakes (Kearney & Kruger, 2016). Compliance with information security policies creates procedures that aid in risk mitigation of employees' behavior (Da Veiga, 2016; Sohrabi et al., 2016; Sommestad, Karlzén, & Hallberg, 2015). Information security culture engages the identifications of security-related ideas, beliefs, and values of the business.

Information security knowledge sharing, collaboration, intervention, and experience all have a significant effect on employees' attitude towards compliance with organizational information security policies (Kearney & Kruger, 2016; Nykänen & Kärkkäinen, 2016; Sommestad et al., 2015). The presence of business leader commitment and personal norms affect employee attitudes. Employee attitude towards compliance with information security organizational policies also have a significant effect on the behavioral intention regarding information security compliance (Sommestad et al., 2015).

Internal auditors and information security management play important roles in protecting an organization's assets (Steinbart, Raschke, Gal, & Dilla, 2013). The two groups are not always supportive of one another. There are definite benefits of the two groups working together. According to Roratto and Dotto (2014), one of the key activities for data loss prevention is an audit. Roratto and Dotto added the importance of having reliable records of activities in order to be able to audit a system. Kanatov, Atymtayeva, and Yagaliyeva (2014) and Steinbart et al. (2013) posited that systems store critical data, whether financial or operational and must have features such as audit log, also called audit trail, which records all activities on data. Recording critical data activity enables the identity of harmful actions that can be internal or external, intentionally or unintentionally caused (Chatterjee et al., 2015; Roratto & Dotto, 2014). Steinbart et al. (2013) reported that the level of technical expertise possessed by internal auditors and the extent of the internal audit review of information security relate to information's security assessment. The quality of the relationship between the internal audit and information security functions is positively associated with perceptions of the value provided by

internal audit and, most important, with measures of overall effectiveness of the organization's information security endeavors (Steinbart et al., 2013). Therefore, special care must occur to protect the integrity of sensitive data adequately. The use of an audit log, also called audit trail, records all activities on critical data which allows for the identity of harmful actions that can be internal, external, intentionally, or unintentionally caused (Chatterjee et al., 2015; Roratto & Dotto, 2014).

Transition

Section 1 of this study included an introduction to the business problem concerning the explorations of strategies some managers implement to manage the risk associated with operational security threats. Technology dependence continues to increase and emerging Internet threats are rapidly growing. Business leaders are finding that security threats produce many challenges and can be detrimental to the success of the business. A discussion of the general problem existing in the areas of rising Internet threat levels, risk management, management objectives, and failures occurred. Literature in the areas of information security culture and information security behavior accompanied literature on workforce development and information security awareness.

Section 2 is a focus on the details of the research project such as the role of the researcher, participants in the study, and data collecting techniques. I also elaborated on the processes and procedures associated with the multiple case study design for data collection strategies. A further objective for Section 2 is to highlight specific strategies to ensure the reliability and validity of the study. In Section 3, I provide research findings, comparing and contrasting the information, and the phenomenon under study with current

literature. I also provided recommendations on the need for future research, and my overall conclusions.

Section 2: The Project

Section 2 contains information on the research design and the research process. The objective of my study was to explore the risk management strategies small business leaders use to prevent and mitigate operational security threats that produce financial losses. In addition, this section includes the purpose statement, the role of the researcher, participants, population, and sampling. The data collection process in this section encompasses the organization, data analysis, and processes for assuring the reliability and validity of my study.

Purpose Statement

The purpose of this qualitative multiple case study was to explore the risk management strategies small business leaders use to prevent and mitigate operational security threats that produce financial losses. The population for this case study consisted of six business leaders from four distinct organizations in South Carolina who have demonstrated successful experience in addressing the specific business problem. Positive social change may include a reduction in financial losses for small businesses, improved profitability, and a reduction in unemployment. The social impact of the study results could affect operational security influencing the success of small businesses, which in turn provides jobs and economic growth to communities.

Role of the Researcher

Qualitative researchers understand the interview process as social interaction (Blythe, Wikles, Jackson, & Halcomb, 2013). Interviews are a means of collecting data in qualitative social research (Anyan, 2013); however, participants must sign an informed

consent form. A requirement of informed consent is advising the participant of his or her protected rights (Nijhawan et al., 2013; Nishimura et al., 2013). The Belmont Report provides the guidance needed, by the researcher, with the study design, ethical principles and guidelines for the participation of human subjects (Fiske &Houser, 2014; Department of Health, 2014). I chose to review the consent form prior to beginning the interview process to minimizes risks and provide any clarity needed by the participants.

The primary data source for qualitative research is the interview process (Marshall, Cardon, Poddar, & Fontenot, 2013). The case study interview protocol (Appendix C) served as a guide and included the following steps: (a) opening statement, (b) semistructured interview questions, (c) probing questions, (d) follow-up questions for clarity, and e) journaling reflexive notes. Using the interview protocol ensures researchers can follow the same process with each participant and adds consistency and reliability to the study (Foley & O'Conner, 2013).

I was the primary collection instrument in the semistructured qualitative interviews, using open-ended questions to conduct face-to-face interviews. No personal or professional association existed between me and the participants, and I facilitated avoiding a potential conflict of interest. My actions remained professional and ethical while probing into the real-life experiences of the participants. In addition, avoiding the use of leading questions through adhering to the interview protocol aided in preventing bias (Yin, 2013). I conducted the research by organizing, observing, analyzing, and interpreting the data collected**.** My objective was to gather detailed descriptions of real-life experiences of the participants on risk management strategies. Using interviews to

collect data enabled participants to think and talk about their experiences and understandings (Anyan, 2013).

To avoid the presence of a personal lens and to mitigate bias, I incorporated member checking, transcript validation, and reflexive journaling. Member checking is a process used by researchers to improve accuracy, reliability, and validity of the findings by allowing participants to validate the content (Harvey, 2015). Participants received a transcript of the interview to check for accuracy in their statements. Reflexive journaling documents the researcher's experiences, thoughts, and concerns (Mackenzie et al., 2013). Hoover and Morrow (2015) defined reflexive journaling as ethically important moments, in which the researcher can reflexively consider the perspectives of participants. Reading the journal allows the researcher returning mentally to the field, with reminders of subtle nuances not necessarily captured in the transcribed data (Mackenzie et al., 2013). Reflexive journaling provides a deeper and more descriptive context of the experience as a whole (Mackenzie et al., 2013). I had no personal or professional connection to the participants or the organizations involved in this study. I avoided any conflicts of interest to ensure my actions remain ethical.

Participants

The targeted population for this case study consisted of business leaders in the organizations comprising the multiple case study who have successfully deployed strategies for preventing cyber security breaches. The sample size of participants for this study consisted of six small business leaders in South Carolina. The participants were a part of effective implementation of risk management strategies to prevent operational

security threats that produce financial losses. Business leaders met the eligibility requirements through implementation of successful strategies in their demographic. The potential participants must be knowledgeable in and understand the dynamics present in the organizational setting and exposure to various security situations over extended periods (De Massis & Kotlar, 2014). Face-to-face, semistructured interviews with participants took place after receiving Institutional Review Board (IRB) approval. I followed Walden University's IRB guidelines to protect the rights of the participants. In adhering to IRB guidelines, all participants signed an informed consent form before the interviews.

I located potential participants through professional associations, the South Carolina Department of Consumer Affairs (SCDCA), and the LinkedIn® online public directory. I used LinkedIn® to recruit potential participants (see Appendix A). I sought the assistance of professional associates to gain access to potential participants. Potential participants, who indicated a willingness to participate, received an e-mail introductory letter (see Appendix D) that outlined my research and the purpose of my study. Establishing a good relationship and building trust with the participants is essential because the participants need to be comfortable responding to questions in an open and honest manner (Doody & Noonan, 2013). Organizations met the eligibility requirements through their demonstrated implementation of successful strategies for preventing or mitigating operational security threats. I conducted an immediate follow-up interview facilitating member checking. I asked the participants to verify that my summaries and

interpretations of the participants' responses to questions were accurate, and if there were any additional information the participants would like to provide.

I applied purposeful sampling to identify potential participants for my study. Purposive sampling strategies are nonrandom sampling methods that ensures participant selection using predetermined criteria (Barratt et al., 2015; De Jaegher, Pieper, Clénin, & Fuchs, 2016; Robinson, 2014). The rationale for employing a purposive strategy is that the researcher needs a certain category of participants who may have a unique, different, or important perspectives on the phenomenon in question (De Jaegher et al., 2016; Elo et al., 2014). I saved data collected and stored on an assigned flash drive. The flash drive will remain locked securely in a safe deposit box for five years, as specified in the participant consent form. After five years, I will destroy the flash drive data to protect the privacy of all participants.

Francis et al. (2010) purposed that researchers test for data saturation by determining a minimum number of sample participants required for the analysis and then designating additional participants to validate saturation. The expected sample size of six was dependent on the point and time in which the data collection reached saturation. According to Dworkin (2012), saturation levels may fluctuate based on elements such as the homogenous level of sampled participants. Data saturation occurs through the conduction of analysis throughout data collection (Elo et al., 2014). To achieve data saturation, I followed Fusch and Ness's (2015) prescribed process that includes: (a) member checking to interpret what the participant shared by confirming the interpretation of information is correct, (b) asking the participant if there is any additional information

available, and (c) continuing the member checking process with all participants until no new information emerges.

Research Method and Design

The three types of research methods are: (a) qualitative, (b) quantitative, and (c) mixed method (Earley, 2014; Moustakas, 1994). I concluded that the qualitative research method, with multiple case study design, was most appropriate for my study based on the nature of the study. Observing participants while gathering information rich data of real-life experiences is a typical additional data source for qualitative multiple case studies (De Massis & Kotler, 2014). Qualitative research is applicable when seeking to analyze key observations that can only come from real life experiences (Birkinshaw, Brannen, & Tung, 2011). According to Bailey (2014), researchers use qualitative methodology to explore and explain human experiences. Researchers develop an understanding of the dynamics within each organizational setting using the case study approach (De Massis & Kotlar, 2014). I interviewed six participants to gain insights into risk management strategies used by small business leaders to prevent operational security threats.

Research Method

O'Brien, Harris, Beckman, Reed, and Cook (2014) and Yin (2014) indicated that qualitative research also contributes to the literature through individual experiences, as they occur in natural rather than experimental situations. Qualitative research is descriptive rather than explanatory, and exploratory rather than testing, revealing individual experiences, relationships, and norms of the business leader (Cottrell & Donaldson, 2013; Cronin, 2014). The strength of the qualitative approach is the

opportunity for flexibility and adaptability throughout the data collection and analysis process (O'Brien et al., 2014).

The research method for this study was qualitative with a multiple case study design. A qualitative method is most effective to gain an understanding of managers' communications with individual employees (Rice et al., 2014). O'Brien et al. (2014) related that qualitative research contributes to the literature in many disciplines by interpreting, describing, and generating theories about social synergy. I explored the different aspects of individual demonstrated objectives to determine how small business leaders use risk management strategies to prevent and mitigate operational security threats that produce financial losses. Managers use qualitative methods to explore in-depth implementation and effective communication (Kamil, Mosenthal, Pearson, & Barr, 2014). Barratt et al. (2013) added that the qualitative research method permits asking questions of selected participants who have actual experiences pertaining to where and how the study phenomenon affects managers. Therefore, qualitative research was the appropriate method for my study.

Quantitative researchers use statistical procedures for examining the relationships and differences among variables (Groeneveld, Tummers, Bronkhorst, Ashikali, & Van Thiel, 2015; Venkatesh, Brown, & Bala, 2013). Using the quantitative method enables researchers to obtain objective answers to questions regarding the what, when, and where relationship to the topic studied (Pettigrew, 2013; Yin, 2013). The quantitative research method occurs primarily in studies that require the researcher to test hypotheses (Birkinshaw et al., 2011). A mixed method was not appropriate for the study due to the

need to employ both quantitative and qualitative approaches in the same study (Venkatesh et al., 2013). I considered both the quantitative and mixed method approaches for my study. Using a systematic procedure to examine the relationships or differences among variables to form conclusions is not pertinent to qualitative studies (Birkinshaw et al., 2011; Groeneveld et al., 2015; Venkatesh et al., 2013). There was no need to consider testing for hypotheses to address my research question; therefore, both quantitative and mixed method designs were not appropriate.

Research Design

The research design for my qualitative study was an exploratory multiple case study. Lewis (2015) categorized qualitative research designs into five groups: (a) phenomenology, (b) ethnography, (c) narrative, (d) grounded theory, and (e) case study. Mayoh and Onwuegbuzie (2013) indicated that phenomenology research designs could be a subjective perspective of the individual experiencing the phenomenon. A phenomenological design can be intense and time consuming (Yin, 2014). With ethnography, researchers observe participants in specific settings for extended periods to understand all aspects involved with groups' cultures (Cruz & Higginbottom, 2013). Using an ethnography design may require researchers to embed themselves into the group to explore the group's culture (Campbell & Scharen, 2013). Lee, Riche, Isenberg, and Carpendale (2015) characterized the focus for narrative design as obtaining data from visually shared stories. Cho and Lee (2014) characterized the purpose for grounded theory design as developing theories for subject phenomena (Hussein, Hurst, Salyers, & Osuji, 2014).

I considered the alternate qualitative designs; however, I elected to use an exploratory multiple case study design for my qualitative study. Case study research is a powerful approach opening new areas while stimulating further research (Cronin, 2014). Cronin (2014) described case study research strategy as one revealing information rich with vivid descriptions. Using the case study design afforded me the opportunity to explore multiple facets of the phenomenon while viewing strategies from a variety of possible lenses (De Massis & Kotlar, 2014). Birkinshaw et al. (2011) and De Massis and Kotler (2014) indicated that a case study provides an excellent means of presenting a phenomenon in real-world contexts. Cronin posited that case study research captures the essence of the researcher's work, from the development of the research question, through the collection and analysis of the data, to the end in completing the concluding paragraphs. De Massis and Kotler added that a case study considers small business development and the strategies implemented throughout various situations and over an extended period. I thus chose a multiple qualitative case study design for this study.

According to Fusch and Ness (2015), data saturation exists for a study if replication of data occurs within the sampled participants. Replication of data occurs when the same information emerges through the addition of interview participants (Toles & Barroso, 2014). I used Fusch and Ness's guidance to achieve and demonstrate that data saturation exists.

Population and Sampling

The population for this multiple qualitative case study consisted of six small business leaders in South Carolina with successful experience in developing and

implementing operational security strategies to prevent and mitigate financial losses. This section includes an explanation of the eligible multiple case study population and sampling that best advanced the study of risk management strategies to prevent or mitigate security threats.

Elo et al. (2014) indicated that there is not a commonly accepted sample size for a qualitative study. Participant emphasis for a qualitative study explores the diversity, rather than the statistical significance of the research (Elsawah, Guillaume, Filatova, Rook, & Jakeman, 2015). I used purposeful sampling for this study. Interviews, observations, and document reviews are part of the validation process of the research in this study (Malterud, 2001). According to Malterud (2001), the qualitative research method involves the systematic collection, organization, and interpretation of textual material derived from talk or observation.

I used the social networking electronic mail service, LinkedIn®, to make my initial introduction to potential participants. The interviews took place at a mutually agreed upon time and location that was comfortable for participants. Positive environments such as private offices, conference rooms, or libraries were possible locations of choice to conduct interviews. Building trust with the participants is essential. The participant needs to be comfortable responding to questions openly (Doody & Noonan, 2013). I confirmed to participants that all documentation from the interview will remain locked securely in a safe deposit box for five years. After five years, document destruction will take place in order to guarantee complete confidentiality of the participants.

In the qualitative research method, achieving and demonstrating data saturation is imperative. The size of the sample should be large enough to achieve reliability and validity (Elo et al., 2014). A test for data saturation occurs by establishing a minimum number of participants required for the analysis (Francis et al., 2010). According to Elo et al. (2014), researchers can perform data analysis throughout the study, allowing them to identify saturation at the point it occurs. The sample of interview participants must be large enough to represent the subject population, but not too large, that the case study becomes overwhelming and unrealistic to complete (Elo et al., 2014). According to Fusch and Ness (2015), there is enough information, and saturation exists for the study, if replication of data occurs within the sampled participants. Replication of data occurs when the same information emerges, through the addition interview participants (Toles & Barroso, 2014).

Six was the number of planned participants for my study. Saturation levels can fluctuate based on elements such as the homogenous level of sampled participants (Dworkin, 2012). After contacting potential participants using purposeful sampling, as needed, I reached out to additional candidates identified during the selection process through LinkedIn®, email, or telephone. Participant recruitment came from business leaders who implemented successful strategies for preventing and reducing security threats.

Patton (2015) described the logic and power of purposeful sampling as information-rich data source selections. With purposeful sampling, the researcher gains considerable insight into issues of paramount importance to the purpose of the

phenomena studied (Anyan, 2013; Patton, 2015). Studying data specific sources yields insights and in-depth understanding of particular issues (Gentles, Charles, Ploeg, & McKibbon, 2015). Perceptions, current practices, and experiences help attain a saturation level of the different ideas (Ishak & Bakar, 2014). Using the data from this research may assist business leaders in identifying operational security risks, providing increased awareness of proposed threats, and reducing financial losses.

Ethical Research

Avasthi, Ghosh, Sarkar, and Grover (2013) and Haahr, Norlyk, and Hall (2013) related that ethics considers the element of understanding the significance of conflicts that arise from moral mandates and the actions taken by those participating in dealing with them. All participants received, via email, an introductory letter (see Appendix D), which described the nature and importance of the research study. Included with the introductory letter was a letter of cooperation (see Appendix B) and a consent form, which disclosed the potential benefits and risks associated with the participation in the study. No incentives, monetary or other, were a part of the participant recruitment process. Although there are no physical risks involved, obtaining an informed consent form prior to interviewing participants is standard protocol (Saunders, Kitzinger, & Kitzinger, 2015).

Saunders et al. (2015) reported that the multitude of new challenges qualitative researchers now face providing anonymity to participants. This emerging problem exists due to the wealth of information once considered private but now readily accessible online (Saunders et al., 2015). To put the participants at ease, I explained the participants'

rights to end the interview or withdraw from the study at any time. A participant was able to withdraw at any time before or during the interview, with no explanation required. If a participant desired to withdraw, they could have done so through contacting me using my email, sending a text, or calling me at the phone number provided in the recruitment letter for study participants (see Appendix A).

To build trustworthiness, as the interviewer, I reviewed the expectations for the participant, and elaborated on confidentiality and ethical responsibilities. The consent form contained an explanation that the data compiled throughout the research will be stored on a flash drive and locked securely in a safe deposit box for five years to protect the rights of participants. After this period elapses, all documents and digital files will undergo destruction in ordered to retain complete confidentiality of the participants.

As a researcher, I followed the protocol of the Belmont Report. The Belmont Report summarizes ethical principles and guidelines identified by the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research for the participation of human subjects in research (Department of Health, 2014). A researcher carefully addresses and includes risks and benefits in the application to the Institutional Review Board (Gennaro, 2014). In addition, ethical research requires IRB approval to precede the interview process. The IRB approval number for this study is 06-30-17-0527045. At the heart of ethical behavior is the need to establish trust between researchers and their participants (Doody & Noonan, 2013). Baker (2013) suggests that researchers may reveal facts that participants do not want or expect to hear.

Participants trust the most, when they believe the researcher will offer them unexpected insights into themselves (Harris & Lyon, 2013).

The foremost principles of ethical conduct are accountability, responsibility, and respect for citizens (Avasthi et al., 2013). As an ethical principle, accountability means to be prepared to answer completely and without hesitation (Jordan, 2014). Accountability is what the intentions are with resources collected and the purpose of the study (Jordan, 2014). Research protocols typically center on four dimensions: (a) privacy and confidentiality, (b) informed consent, (c) protection of vulnerable groups, and (d) the avoidance of harm (Barker, 2013). Therefore, the final doctoral manuscript will not include the names or any other identifiable characteristics connecting individuals or organizations to the study (Barker, 2013).

Data Collection Instruments

Many qualitative design approaches include a definitive protocol involving data collection and data representations (Sousa, 2014). As the researcher, I was the primary data collection instrument. I collected data through semistructured interviews, observations, archived records, and historical information from participants. I requested access to, and use, any secondary data sources offered, demonstrating successful risk management operating procedures. I did not conduct a pilot test of the interview questions. Contrary to unstructured interviews, semistructured interviews involve the use of predetermined questions, keeping the dialog focused on the theme or topic of the study (Birkinshaw et al., 2011; Mitchell, 2015). One of the best tools for researchers is the semistructured interview because it enables the participant to describe current practices

and real-life experiences (Anyan, 2013; Birkinshaw et al., 2011; De Massis & Kotler, 2014; Mitchell, 2015). Participants responded to semistructured interview questions (see Appendix C). Using semistructured interviews permits researchers to deviate from scripted questions to seek clarification (Doody & Noonan, 2013). Researchers using semistructured interviews can gather more insightful information with follow-up questions in pursuit of clarity (Doody & Noonan, 2013). However, participants were able to discontinue the interview process at any time, if they felt a need to do so.

I also incorporated reflexive journaling into the data collection process. Using reflexive journaling enables researchers to mitigate personal bias and beliefs throughout the qualitative research process (Mackenzie et al., 2013; Yu, Abdullah, & Saat, 2014). However, Yu et al. (2014) explained that a complete detachment of a researcher's personal perceptions is impossible. The use of reflexive journals increases the researcher's ability to remain neutral toward the phenomenon under study (Ponterotto, 2014). Hoover and Morrow (2015) indicated using reflexive journaling identifies ethically important moments, in which the researcher can reflexively consider the perspectives of participants. Reading the journal reminds the researcher of subtle nuances not always incorporated into the transcribed data (Mackenzie et al., 2013). Mackenzie et al. (2013) posited that reflexive journaling provides a deeper and more descriptive context of the experience and documents the researcher's experiences, thoughts, and concerns. Hoover and Morrow further defined reflexive journaling as, ethically important moments, in which the researcher can reflexively consider the perspectives of participants. Reading the journal allows the researcher to return mentally to the field,

with reminders of subtle nuances not necessarily captured in the transcribed data (Darawsheh, 2014; Mackenzie et al., 2013).

There are various methods for increasing the reliability and validity of interviews. A significant method for achieving reliability and validity is recording participant interviews. I used a Sony Digital Voice Recorder to document the interview and to validate credibility. Recorded interviews improve reliability and validity because researchers can progressively check recordings for accuracy and validity (Al-Yateem, 2012). Yin (2014) stated that researchers could enhance the reliability and validity of case studies by using multiple data sources for methodological triangulation. Yin related that case study research allows the researcher to collect data from additional sources that may include historical documentation and archived records.

I used methodological triangulation analyzing and compared the results of the interviews, observations, archived records and historical information. I requested access to, and used any secondary data sources offered, regarding standard risk management operating procedures. The review of transcripts enhanced reliability and validity using member checking. Member checking is a process used by researchers to improve accuracy, reliability, and validity of the findings reported by allowing participants to validate the content (Harvey, 2015). I provided participants with a written transcript to validate the content and check for resonance with their experiences.

Data Collection Technique

I made initial contacts to participants who met the criteria of my study through LinkedIn® electronic mail service. A phone call to potential participants responding with

interest and a willingness to participate took place to form a working relationship. Discussions include the expectations for participants, the confidentiality and ethical responsibilities of the researcher, and a convenient time and location to meet (Barker, 2013). I emailed a copy of the Informed Consent Form to participants for review prior to arrival. Lewis (2015) recommended opening the scheduled interview with a review of the consent form to assure the terminology and intent are clear. I informed potential participants that the interview would take up approximately 60-minutes, unless participants chose to extend the time for more discussion. Doody and Noonan (2013) suggested making the participants aware that, at any time during the interview, the interview may cease at the participant's choosing.

A semistructured interview occurred using the six interview questions (see Appendix C). I used a Sony Digital Voice Recorder to document the interview in an efficient manner. The use a recording device is a valuable tool in the research process, ensuring reliability and validity of the conversations (Al-Yateem, 2012). The use of TranscribeMe® software created a transcription of the interviews. Transferring transcribed information into QSR NVivo® aided me in organizing the data. With the use of QSR NVivo® software, proper coding of topics for analysis transpired. Appropriate data analysis is vital and begins with listening to relevant statements while emphasizing the significance to the researched phenomena (Moustakas, 1994). Each participant had the ability to receive a copy of the study summary.

Qualitative semistructured face-to-face interviews also offer a distinct advantage in providing social cues such as voice, intonation and body language (Irvine, Drew, &

Sainsbury, 2013). The semistructured interview is one of the best tools for researchers to elicit the entire narrative about the perceptions of participants (Mitchell, 2015). According to Doody and Noonan (2013), a bond establishes with participants, building a rapport that allows asking more in-depth follow-up questions by the researcher. With face-to-face interviews, the researcher can see if the interviewee presents signs of discomfort or distress provoked by the line of enquiry (Irvine et al., 2013). The disadvantages of face-to-face interviews are that they may be obtrusive (Doody & Noonan, 2013).

I used member checking to ensure the accuracy of reported findings. Member checking, also known as participant or respondent validation, is a technique used by researchers to aid in improving accuracy, reliability, and validity of the findings provided by the participant (Birt, Scott, Cavers, Campbell, & Walter, 2016; Harvey, 2015). When conducting member checking, data confirmation occurs to check for resonance with their related experiences (Birt et al., 2016; Blythe et al., 2013). I implemented member checking by providing the participant with a written transcript, allowing the participant to validate the content. I followed up with each participant to confirm that the reported findings align with that communicated during the interview.

I implemented a method referred to as epoche, which used the semistructured interviews to validate the study. Moustakas (1994) indicated epoche is a technique to mitigate bias that may take place in the phenomena studied. Awareness of potential bias is imperative to the success of the study. The researcher must have the ability to set aside such bias in order to view the phenomena from a fresh perspective. Academic rigor

increases when the researcher applies epoche throughout the project (Yu et al., 2014). To mitigate bias and presumptions, Ponterotto (2014) stated that participants must not be colleagues or individuals known personally in any other manner. I had no personal or professional connection to the participants or the organizations included in this study.

In addition to semistructured interviews and observations, archived records and historical information were supplemental data types for my study. Researchers use qualitative case studies to collect data from multiple sources with a viable source being documentation from archived records (Cope, 2014; Gioia, Corley, & Hamilton, 2013; Yin, 2014). Collecting documentation from historical information and archived records is advantageous due to participants having access to company management strategies that otherwise would not be available through public records (Bryde, Broquetas, & Volm, 2013). The disadvantage of using such methods of data collection is the potential increase in subjectivity. Bryde et al. (2013) added that it is feasible to find information that may be out of date, incomplete, or inaccurate. I therefore, considered the advantages of requesting supporting documentation to which, otherwise, I would not have had access. I asked each participant if standard risk management operating procedures are available to help support the prevention of operational security risks. I verified that the contents of supporting documentation, aligned with the information from interviewing the participants. Yin (2014) stated that the use of multiple sources enables the triangulation of the data collected in the interviews and secondary data.

Data Organization Technique

Valid, reliable, and precise qualitative research starts with a scrupulous organization of the data collected (Gioia et al., 2013). Pierre and Jackson (2014) stated that organizing raw data in a straightforward form makes analysis easier for the researcher. The use of QSR NVivo® software aided in the organization of interview data. The interview documents included a heading to identify each interviewee. For example, I identified business leader one as BL1 and the headings continued sequentially. I used a technique involving a reflexive electronic journal focusing on the reasons for undertaking the research. A reflexive journal is another form of bracketing (Lincoln & Guba, 1985) and I used a reflexive journal from the beginning of the research process.

Campbell (2013) explained that the use of coding to organize data aids the researcher in the discovery of enhanced topics. The coding technique is preferred method used by researchers for organizing raw data in a straightforward form for easier analysis (Pierre & Jackson, 2014; Rosenfeld, Gatten, & Scales, 2013). I used QSR NVivo® to organize the topics from interviews, observations, archived records, historical information, notes and journaling recorded throughout the research process. This organizational technique allowed the cross-analysis of data from all sources and an analysis of each source individually (Pierre & Jackson, 2014; Rosenfeld et al., 2013). I saved any transcripts of data collected along with any QSR NVivo® coded data in this process on an assigned flash drive. The flash drive will remain locked securely in a safe deposit box for five years. After five years, I will destroy the flash drive to protect the privacy of all participants.

Data Analysis

Triangulation aids the researcher in the reduction of bias and cross-examining participant response to affirm integrity (Anney, 2014). The triangulation method assures and demonstrates reliability, confirmability, and credibility of the study's findings (Houghton, Casey, Shaw, & Murphy, 2013). Carter, Bryant-Lukosius, DiCenso, Blythe, and Neville (2014) explained the four forms of triangulation: (a) data triangulation, (b) investigator triangulation, (c) theoretical triangulation, and (d) methodological triangulation. I used methodological triangulation for my study. The multiple methods of data collection in methods triangulation are important in articulating the comprehensive view of a phenomenon (Carter et al., 2014; Cope, 2014). Methodological triangulation involves the use of multiple types of data in studying a phenomenon (Bekhet & Zauszniewski, 2012; Wijnhoven & Brinkhuis, 2015). Methods of data collection can include interviews, observation, archived records, historical information, notes and journaling recorded throughout the research process (Cope, 2014). I analyzed the data from all sources, both individually and comparatively, to assure and demonstrate academic rigor, reliability, and validity.

Using software analysis tools enables researchers to attain a deeper analysis of collected data (Woods, Paulus, Atkins, & Macklin, 2015). I analyzed the recorded interviews and transcriptions using Moustakas' (1994) modified van Kaam method of analysis and the QSR NVivo® research software. Moustakas applied a seven-step modified van Kaam analysis method allowing researchers to analyze textual data. The modified van Kaam analysis steps included: (a) grouping textual data listings, (b)

eliminating proportional topics of the phenomenon, (c) clustering core topics, (d) checking for inconsistencies in the flow of the interview transcript, (e) developing a structured description of experiences by each person, (f) creating a structured description based on the textual data, and (g) implementing an individual textural-structural description of the data from the combined interviews (Moustakas, 1994). I applied the seven-step modified van Kaam analysis throughout the data analysis process of my study.

According to Campbell (2013), the use of coding to organize data aids the researcher in the discovery of enhanced topics. QSR NVivo® is a software application that allows researchers to code topics for easier analysis. The coding technique is a preferred method of organizing raw data in a manner that makes analyzing easier (Pierre & Jackson, 2014; Rosenfeld et al., 2013).

I used QSR NVivo® to identify emerging topics from interviews, observations, archived records, historical information, notes and journaling recorded throughout the research process. Using this organizational technique enables the cross-analysis of data from all sources and an analysis of each source individually (Pierre & Jackson, 2014; Rosenfeld et al., 2013). The use of QSR NVivo® allows the researcher to group the coded data into topics to identify key themes and correlate the key themes with both the conceptual framework and literature.

Reliability and Validity

Researchers face major challenges in acquiring high-quality data when conducting and reporting research (Cope, 2014). Dependability, creditability, transferability, and confirmability are techniques for assessing and demonstrating the

reliability and validity of qualitative research (Cope, 2014; Franco, Mannell, Calhoun, & Mayer, 2013; Houghton et al., 2013). Houghton et al. (2013) elaborated that the transparency of the data analysis processes assures academic rigor, reliability, and validity.

Reliability

Reliability allows for reproduction of results (Vaz, Falkmer, Passmore, Parsons, & Andreou, 2013). Reliability links reproducibility and stability to the data collected (Franco et al., 2013). Guidelines crafted as an interview protocol ensure reliability before, during, and after the interview process. The detailed research question is the guiding factor in the achievement of dependability. Data saturation becomes evident when any new data collected no longer add new or relevant information to the study (Dworkin, 2012). When responses given by participants become redundant, the researcher has achieved data saturation. Dependability refers to the ability to repeat the study in the same conditions (Kallio, Pietila, Johnson, & Kangasniemi, 2016). Franco et al. (2013) confirmed that dependability and reliability occur **t**hrough the detailed description of the conceptual framework, the role of the researcher, participants, research method, research design, data collection, and data analysis. Such detailed descriptions ensure that the readers understand the study's foundation (Anyan, 213; Kallio et al., 2016). In presenting the complete interview protocol (see Appendix C) of the development process, I enabled other researchers to review and understand the basis for my study's conclusions.

The use of member checking further enhanced dependability, ensuring the accuracy of reported findings. Member checking, also known as participant or respondent

validation is a technique for exploring and assuring the credibility of results (Birt et al., 2016). Data or results returns to participants to check for accuracy and resonance with their experiences (Birt et al., 2016). I provided the participants with a written transcript of their interview to confirm complete understanding of the ideas that the participant intended to convey and the accuracy of my interpretations. I followed up with each participant to confirm ideas and communication are appropriate. The participants had the opportunity to correct or clarify any information reported in the transcript through my use of member checking.

Validity

Credibility refers to the trustworthiness of the research (Erlingsson & Brysiewicz, 2013; Yilmaz, 2013). I used a digital voice recorder to document the interview and to assure credibility. The use of a recording device is a valuable tool in the research process, improving credibility enabling the researcher to check recording continuously for efficiency as the interview is transcribed (Al-Yateem, 2012).

Using triangulation serves to confirm findings' validity and to ensure the data are complete (Houghton et al., 2013). Using methodological triangulation further strengthens credibility. Methodological triangulation is a technique that enables the researcher to improve the rigor of qualitative research by comparing and contrasting various types of data (Bekhet & Zauszniewski, 2012; Houghton et al., 2013). The compilation of data for the study came from interviews, observations, archived records, historical information, notes and journaling recorded throughout the research process. I used methodological data triangulation by comparing the findings and conclusions from each data type to

assure the findings' validity. I reviewed secondary documents and my reflexive journal to triangulate and confirm the findings from the data sources.

I further demonstrated credibility by ensuring data saturation occurred. Data saturation takes place when collecting additional data adds no new information to the conversation (Dworkin, 2012). I chose six as my participants but tested for data saturation throughout the process. Data saturation takes place through the conduction of analysis throughout data collection (Elo et al., 2014). The importance of data saturation in qualitative research means giving full expression to the values desiring to communicate through the research (Gergen, Josselson, & Freeman, 2015). The interview and member checking process continued until the achievement of data saturation occurs. Oberoi, Jiwa, McManus, and Hodder (2015) concluded that data saturation is a decision point where the researcher affirms that there is no further need to collect data. Kallio et al. (2016) stated confirmability of the study refers to demonstrating the researcher's objectivity Researchers can demonstrate confirmability by clearly describing the data collection process and making the overall research process as transparent as possible (Kallio et al., 2016). I used member checking to assure confirmability. Using member checking enables the researcher to validate the content of the transcribed interview (Harvey, 2015). Returning the transcribed results to participants to confirm resonance with their experiences implements member checking and aids in assuring confirmability (Birt et al., 2016; Blythe et al., 2013).

Transferability in qualitative research is equivalent to external validity in quantitative research (Erlingsson & Brysiewicz, 2013; Houghton et al., 2013). The

researcher accomplishes transferability through comprehensive depictions of population, sampling, and demographical processes for the study. The comprehensive explanation of the processes for obtaining and assuring information-rich data presented in the study enables other researchers to determine transferability (Cope, 2014; Erlingsson & Brysiewicz, 2013).

Transition and Summary

Section 2 contained a comprehensive explanation of the research design and data analysis process. I identified the role of the researcher in the project, participants, research method and design, populations and sampling, data collection instruments, data collection technique, data organization technique, data analysis, and means for demonstrating the study's reliability and validity. Section 2 detailed the need for, and means for, assuring ethical research and its intrinsic value. Ethical conformity is vital to ensure confidentiality and to protect the rights of participants. The data collection techniques assure academic rigor, reliability, and validity throughout the study. In Section 3, I focus on the actual outcomes of the research including findings, implications, and results from reflections. I provide detailed descriptions and analysis of participants' interview responses to address the underlying research question. Additionally, Section 3 includes applications for professional practice, recommendations for action, further research, implications for social change, and my overall conclusions.

Section 3: Application to Professional Practice and Implications for Change

Introduction

The purpose of this qualitative multiple case study was to explore the risk management strategies small business leaders use to prevent and mitigate operational security threats. The population for this study consisted of six business leaders in South Carolina who were a part of an effective implementation of risk management strategies that prevent and mitigate operational security threats. Company documents pertaining to security procedures, audits, and reviews, along with interview data and site observations, provided the basis for confirming findings through methodological triangulation. There were four core emergent themes from the research: (a) operational security training and awareness, (b) operational security culture and behavioral effects, (c) operational security policy and compliance, and (d) operational security challenges and risk management.

In Section 3, I provide the findings of the study to explore the risk management strategies small business leaders use to prevent and mitigate operations threats that produce financial losses. Section 3 also includes the application to professional practice and implications for social change. Additionally, Section 3 includes recommendations for actions and for further study, reflections, summary, and my conclusions.

Presentation of the Findings

The overarching research question for this study was: What risk management strategies do small business leaders use to prevent and mitigate operational security threats that produce financial losses? Data collection consisted of semistructured interviews with each participant and the collection of company documents that pertained

to security procedures, audits, and reviews. I used the case study interview protocol (see Appendix C), and analyzed the recorded interviews and transcriptions using Moustakas's (1994) modified van Kaam method of analysis and the QSR NVivo® research software to identify emerging topics. The four themes that emerged from my analysis were: (a) operational security training and awareness, (b) operational security culture and behavioral effects, (c) operational security policy and compliance, and (d) operational security challenges and risk management. In the following headings, I identify the findings relative to each theme, how each of the themes aligns with the literature, and the extent to which each theme supports the conceptual framework of transformation leadership theory.

Theme 1: Operational Security Training and Awareness

The first theme to emerge during data analysis was the importance of developing and maintaining a strong security culture through training and awareness. The lack of information security awareness, ignorance, negligence, apathy, mischief, and resistance are the root causes of user mistakes (Safa, Von Solms, & Furnell, 2016). Hardware and software security mechanisms strengthen IS against attacks. However, these systems are still highly vulnerable to threats from users' undesirable behaviors, which are closely related to IS users' information security awareness (Öğütçü, Testik, & Chouseinoglou, 2016). Participants stressed the need to develop an innovative approach to prevent and mitigate emerging operational security threats. The approach would require business leaders to provide continuous training and threat awareness programs. Participants agreed that keeping staff aware of current security issues are important in establishing strong

threat prevention and mitigation. Participants all concurred, in the statements below, that training was imperative.

- BL1: “I show them what the viruses look like and how to spot them. In a test database, I can show them when they are infected and what to look for.”
- BL2: “It’s a federal requirement that we do training. We train on privacy and the security components monthly.”
- BL3: “If the staff has questions, they screen shot it or take a picture with their phone and send it to me and say is this a scam? If it is bad, I will send an email to everybody and tell them, so-and-so got this on their computer, do not open! We keep everyone informed, that is the key.”
- BL4: “We cannot control what other people do, but we do try to educate our staff and our customers on things that can happen.”
- BL5: “Our reputation is extremely important, the key to educating as many folks as possible. Just keep going back over things again and again. We take the opportunity to reiterate things of importance at periodical gatherings that we have; meeting, luncheons, special functions, things like that.”
- BL6: “Training and keeping staff aware of current security issues are important to establishing a strong security culture.

The emergent results interpreted from the conceptual summaries in Table 2 focused on participants’ responses to operational security training and awareness. Based on the coded responses of the business leaders and the review and analysis of company documents, there were 140 total mentions from the participants’ interviews referencing

the theme of operational security training and awareness. Table 2 displays the subthemes and frequencies.

Table 2

Frequency of Operational Security Training and Awareness

Subtheme	*N*	% frequency of occurrence
Training	36	26%
Educate	50	36%
Communicate, talk, question	54	38%

Note. N = the frequency that each subtheme was mentioned across all participants.

Comparisons of findings from Theme 1 with the literature. The participants' response data show that attending to information security training and awareness can positively affect the information security culture and enhances the culture over time. Previous researchers on information security training and awareness have focused on informing employees about security policies and the penalties for violating those policies. According to Barlow, Warkentin, Ormond, and Dennis (2013), sanctions may not be the most powerful influencer of employees' violations. Da Veiga and Martins (2015) argued that the human element and employee behavior gives direction through the implementations of corrective actions. Participants agreed with AlHogail and Mirza (2014)' s findings that that cultural enhancements in perceptions, attitudes, values, assumptions, and knowledge guide the human interaction when interacting with IS. Therefore, to achieve a successful security component, keeping employees informed, trained, and aware of exposure and consequences, is vital. According to Tsohou, Karyda, and Kokolakis (2015), standards and best practices for information security awareness

programs focus on the content and processes of the programs without taking into consideration how individuals internalize security related information and how individuals make security-related decisions. The findings of the study concur with Tsohou et al. (2015)'s findings that expand on security culture and behavior as a primary consideration by business leaders in workforce development. Information security behavior, improving employee performance, and developing the workforce to its fullest potential are a primary focus in the development of a more potent security solution (AlHogail & Mirza, 2014).

Comparison of Theme 1 findings with those expected from the conceptual framework. Stone et al. (2004) defined transformational leadership theory as an attempt by leaders to succeed in raising followers to a greater awareness. The increased awareness helps business leaders remain focused on the issues of consequence. Transformational leaders seek to transform individual goals into a joint vision for the entire team (Braun et al., 2013). I therefore concluded that the training strategies supported the Burns (1978) and Bass (1985) theories of transformational leadership.

Theme 2: Operational Security Culture and Behavioral Benefits

There were 66 total mentions from participant interviews referencing the theme of operational security culture and behavioral effects. The specific mentions occurred across three subthemes. Table 3 displays the subthemes and the associated total frequencies with which the participants mentioned each subtheme.

Table 3

Frequency of Operational Security Culture and Behavioral Effects

Subtheme	*N*	% frequency of occurrence
Behavior, intent	19	29%
Culture, setting	22	33%
Effect, influence	25	38%

Note. N = the frequency that each subtheme was mentioned across all participants

Comparisons of findings from Theme 2 with the literature. Security culture reflects the values and beliefs of information security shared by all members at all levels of the organizations (D'Arcy & Greene, 2014). Participant comments align with D'Arcy, Herath, and Shoss (2014) findings that leaders set the stage for the culture in which they wish to operate. D'Arcy et al. advocated that promoting security culture as an important factor in maintaining an adequate level of information security in organizations. The contention is that significant efficacious changes in security culture can reduce the number of security breaches experienced. Participant responses showed leading by example is important for security culture and affects the behavior of employees.

Assessment of information security cultures takes place by using an approach such as an ISCA (Da Veiga & Martins, 2015). The empirical data derived from an ISCA might influence the information security culture by focusing on critical developmental areas through awareness and training programs (Da Veiga & Martins, 2015; Line & Albrechtsen, 2016). Da Veiga and Martins (2015) illustrated that the theoretical ISCA tool may include implementation in organizations to influence the information security

culture in a positive manner. Da Veiga and Martins further posited that there is empirical evidence indicating that information security training and awareness is a significant factor in positively influencing an information security culture when applied in the context of ISCA.

According to Kearney and Kruger (2016), the three main organizational groupings (management, technology, and users) displayed in Figure 3 are interdependent and interact with each other.

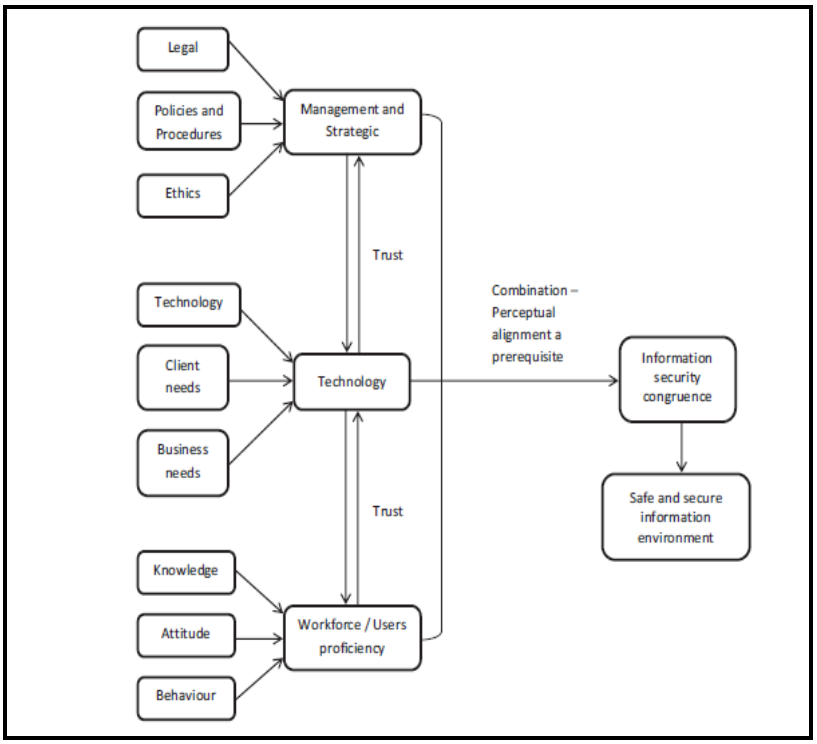


Figure 3. Safe and secure environment model. Adapted from "Can Perceptual Differences Account for Enigmatic Information Security Behaviour in an Organisation," by W. Kearney and H. Kruger, 2016, *Computers & Security*, *56*, p. 68. Copyright 2015 by Elsevier Ltd.

Although other factors exist, trust remains one of the more significant (Kearney & Kruger, 2016), and governs this interaction. Information security behavior, improving employee performance, and developing the workforce to its fullest potential are a primary focus in the development of a more potent security solution (AlHogail & Mirza, 2014; Chatterjee, Sarker, & Valacich, 2015; Flores & Ekstedt, 2016; Montesdioca & Maçada, 2015; Northouse, 2015). D'Arcy and Greene (2014) reported that a well-defined process of security communication leads to an increase in acceptable and proactive user actions regarding information security. Processes that involve education, reminders and refresher courses increase employee feelings of responsibility and ownership in decisions about information security (D'Arcy & Greene, 2014). To reach a point where information security will prevail, Kearney and Kruger (2016) stated that the three groupings shown in Figure 3 must intertwine. A crucial requirement for a successful combination of the groupings is that the perceptions and views of all management, technology, and users should be aligned (Kearney & Kruger, 2016). The alignment will result in a form of information security congruence that provides the desired results, a safe and secure information environment (Kearney & Kruger, 2016).

Comparison of findings from Theme 2 with the transformational leadership conceptual framework. Implementing transformational leadership theory requires leaders with vision, self-confidence, and inner strength that campaign for what they see is right or good, not for what is popular or is acceptable (Kuhnert & Lewis, 1987). Kearney and Krugar (2016) established that trust is the key component to positive interaction between leaders and employees. Participants' responses noted in Table 3 related to the

conceptual framework of my study and the findings from previous researchers (AlHogail & Mirza, 2014; Chatterjee et al., 2015; Flores & Ekstedt, 2016; Montesdioca & Maçada, 2015). In addition, Breevaart et al. (2014) characterized transformational leadership by the four I's: (a) idealized influence, (b) inspirational motivation, (c) individual consideration, and (d) intellectual stimulation. Idealized influence is followers identifying with their leaders and respect and trust them (Breevaart et al., 2014). Inspirational motivation refers to creating and communicating an appealing vision of the future and to the leader's own optimism about the future (Breevaart et al., 2014). Next, individual consideration means that leaders are mentors and acknowledge that every employee has their own specific needs and abilities (Breevaart et al., 2014). Finally, intellectual stimulation is challenging followers to rethink some of their ideas and to take a different perspective on the problems they face in their work (Breevaart et al., 2014). The following quotes from participants during the interview process, confirmed the importance of the four I's which define how employees perceive management:

- BL1: "The best strategy we have is just training, changing the culture in the company."
- BL2: "Always be prepared, expect the worst and hope for the best. Stay in tune with what is going on in the world with regard to information security among other things."
- BL3: "We are constantly training on security issues, and now they will forward questionable things to me to look at, and ask if it is okay."

- BL4: “The older customers seem to be more gullible, but at the same time the younger are more readily to adapt to any type of new technologies and that is scary.”
- BL5: “I try and explain to our employees that it is a culture change, the restrictions are to protect us all. We can be completely trusting and all on the same page, but someone else could take advantage of that.”
- BL6: “Leadership must set the example, led by example, setting the stage for the security culture that we want our employees to operate in.”

A business is most vulnerable when the operating system consists of weaknesses exploited by predators seeking information that may result in negative effects (Jouini, Rabai, & Aissa, 2014). When vulnerabilities exist in a system, security threats manifest via a threat agent or hacker using a particular infiltration technique that can cause undesired effects (Jouini et al., 2014). The financial loss to businesses due to security threats could be significant. Jouini et al. (2014) indicated that losses caused by viruses, unauthorized access, and theft of laptop, mobile hardware, and proprietary information were 74.3% of total losses. In addition, Jouini et al. reported that 70% of fraud occurs with insiders, rather than by external criminals, but 90% of security controls focus on external threats. The findings of my study show the need for a positive organizational culture surrounding information security. A positive and informative culture may have an effect on employee behavior and positively influence security outcomes.

Theme 3: Operational Security Policy and Compliance

Table 4 displays the subthemes presented during participant interviews. There were 72 mentions that correlated with the theme Operational Security Policy and Compliance. Three categories comprised the subthemes.

Table 4

Frequency of Operational Security Policy and Compliance

Subtheme	*N*	% frequency of occurrence
Compliance	16	22%
Policy, procedure	25	35%
Implement	31	49%

Note. N = the frequency that each subtheme was mentioned across all participants.

Information security breaches lead to unexpected additional costs for organizations (Safa et al., 2016). Proper information security behavior mitigates the risk of information security breaches in organizations (Safa et al., 2016). Participants revealed that a particular set of standards is required to instill a culture of compliance.

- BL1: "We have to set a standard, a shift to a culture of compliance."
- BL2: "You have to monitor, stay on top of things, you have to track and trend."
- BL3: "We have an outside consultant group that monitors, and I monitor also."
- BL4: "We have compliance training twice a year, we send newsletters, and periodically we send reinforcement, like reminder emails and such."

- BL5: “We have an in-house IT manager and an IT network security consultant. Together they work in tandem, monitoring activity and looking out for things to come.”
- BL6: “We believe that making end users aware of the monitoring and continuing to stress policy and procedures have a positive impact on compliancy.”

D’Arcy and Greene (2014) examined the influence of security-related and employment relationship factors on employees’ security compliance decisions. A major challenge for organizations is encouraging employee compliance with security policies, procedures, and guidelines. D’Arcy and Greene reported that security culture, job satisfaction, and perceived organizational support have a positive effect on employees’ security compliance intentions. Employees want to be *in the know* and leaders have the capability of creating a culture of transparency through informative actions. However, managers must consider employees’ intent when sharing formative actions. Security experts concluded through documented cases that employees are the weakest link in information security defenses (Chatterjee et al., 2015).

Comparisons of Theme 3 findings with the literature. Information security policy provisions incorporate guidelines for employee reference when interacting with IS to business leaders (Da Veiga, 2016). The lack of security of the Internet and the devices connected to IS results in serious vulnerabilities (Hill, 2015). Violating information security policies is a common problem for most businesses. Violations experienced by businesses range from sharing passwords with coworkers and others who have access privileges to financial losses through the abuse of workplace technologies (Willison &

Warkentin, 2013). The threat of an organizational insider is one of the greatest concerns of information security managers. Regrettably, there are documented cases of employee intentional and nonintentional noncompliance with information security policies (Chatterjee et al., 2015). Evidence suggests that a preponderance of information security incidents occur driven by trusted employees' actions (Crossler et al., 2013; Sikolia, 2013).

Workplace training and exposure also provide employees with the skills, knowledge, and resources, which can enable them to implement successful computer abuses (Willison & Warkentin, 2013). Figure 4 shows sources, perpetrators, and the intent of information security violations. Knowledge of security loopholes exploited by rogue employees through the access of computing resources provided by the organization may have devastating effect (Willison & Warkentin, 2013). Ethical beliefs held by the individuals, along with economic, social, and technological considerations are relevant to security compliance intentions (D'Arcy et al., 2014). In terms of practical implications, D'Arcy et al. (2014) suggested that multiple interventions at various levels may be required to combat growing security threats.

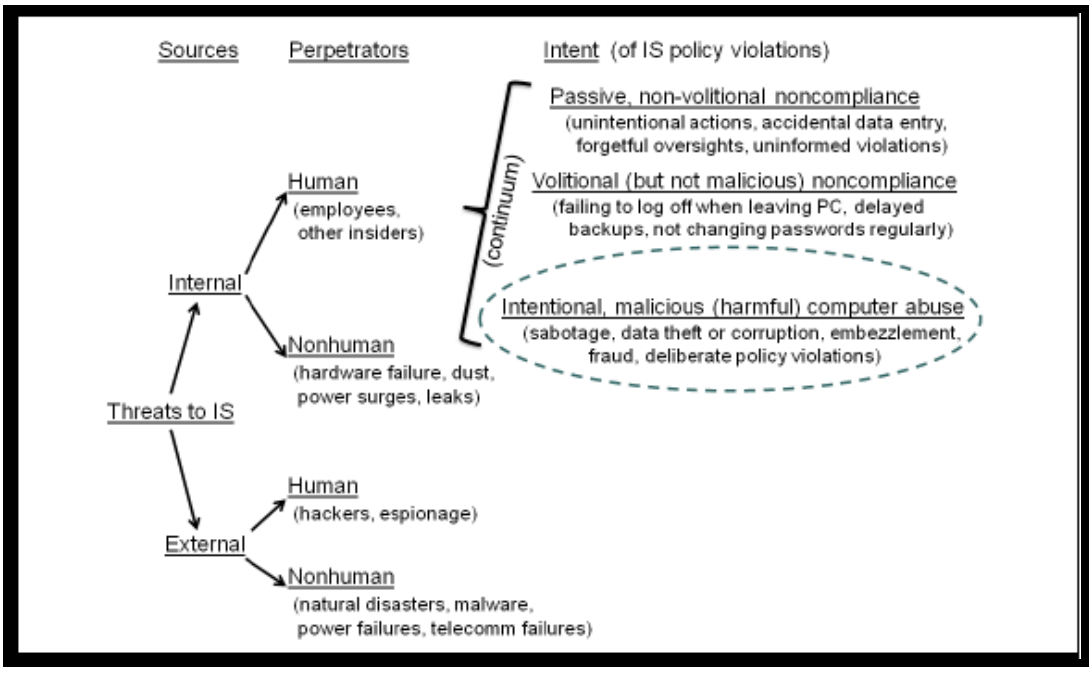


Figure 4. Employee computer abuse. Adapted from "Beyond Deterrence: An Expanded View of Employee Computer Abuse," by R. Willison and M. Warkentin, 2013, *MIS Quarterly, 37*, p. 3. Copyright 2013 by Alok Gupta Publishing.

Comparison of findings for Theme 3 with the transformational leadership conceptual framework. A major challenge for organizations is encouraging employees to follow mandated information security policies, procedures, and guidelines (Darcy et al., 2014). Many employees routinely make a conscious decision to violate such mandates because they want to expedite their work or falsely increase personal productivity (Darcy et al., 2014). Other employees use more harmful intentions such as stealing sensitive corporate data or sabotaging company networks (Darcy et al., 2014). Regardless of intent, Darcy et al., (2014) indicated that over half of all information security breaches stem from employees' lack of security compliance. Willison and Warkentin (2013) presented in Figure 4 violations that

generally fit with the volitional, but nonmalicious, actions of employees. Such violations, although significant, are often dwarfed by a major insider abuse event that has an exacerbating cost impact to the business (Willison & Warkentin, 2013).

Transformational leadership is an attempt by leaders to implement raising follower awareness of potential consequences from poor decisions (Stone et al., 2004). Follower performance improves through transformational leadership and can help develop employees to their fullest potential (Northouse, 2015). Transformational leadership challenges followers to explore new ways to develop and implement management strategies (Northouse, 2015). Strategic management theories, leadership, operational controls, and accountability provide the composite conceptual framework for my study (Braun et al., 2013). Transformational leaders seek to change individual goals into a joint vision for the entire team and develop an innovative approach to emerging operational security threats (Braun et al., 2013). The findings of my study therefore align with expectations from the conceptual framework and build on the antecedents of employees' security compliance.

Theme 4: Operational Security Challenges and Risk Management

Strategic business development and the discovery of new business threat opportunities presents challenges and requires the implementation of innovative risk management strategies (Ramayah et al., 2015). Participants showed resilience throughout the interviews for adapting to a changing culture by implementing effective risk management stratigies. Table 5 displays participant results from interviews and company documents for subthemes of operational security challenges and risk management.

Table 5

Frequency of Operational Security Challenges and Risk Management

Subtheme	*N*	% frequency of occurrence
Monitor, breach	35	15%
Manage, strategy	54	23%
Time, response	55	24%
Challenge, risk	87	38%

Note: N = the frequency that each subtheme was mentioned across all participants

Small businesses are the backbone to economic development and employment growth (Ramayah, Ling, Taghizadeh, & Rahman, 2015). Small business leaders are hesitant to embrace and adopt new technology (Dahnil, Marzuki, Langgat, & Fabeil, 2014). Reluctance of small business leaders could suffer from resource poverty compared to large companies (Dahnil et al., 2014). Other than resource poverty, challenges that face small businesses include organization structure, number of employees, and company culture all of which may cause low technology adoption levels (Ramayah et al., 2015). Having the ability to anticipate the risks that may be forthcoming is a challenge for all businesses. Participants expressed the importance of risk assessment.

- BL1: "The challenge is the scope of the issues; it is just again, getting the information out there to people who need it."
- BL2: "One of the greatest challenges for managers is persuading the governing body of the security needs to keep everything in place to mitigate risks. Risk

assessment is important, and the ability to anticipate the risks that may be forthcoming."

- BL3: "You have to think like them, what would be the smart way, to be bad! The challenge to them is to see how far they can go and the challenge for us is to think ahead."
- BL4: "We are always looking at new software that will help mitigate any kind of breach in security of any kind. We are continually exploring new avenues as technology evolves."
- BL5: "We need to ask ourselves, who is our person out there watching the coming trends. It may not seem necessary now, but it will be vital to mitigating security risks of the future."
- BL6: "there are governmental regulations that have to be implemented; it is always a juggling act, where do your dollars need to go to mitigate risks. Where are they best spent?"

Comparisons of findings from Theme 4 with the literature. With the vast development of information technologies and increasing accessibility to the Internet, organizations become vulnerable to various types of threats (Jouini et al., 2014). All participants agreed that being prepared to combat threats is vital. One of the greatest challenges that businesses face is the response time to rising Internet threats (Shin et al., 2013). Business leaders must act promptly, while accurately predicting the period and severity of threats (Shin et al., 2013). Organizations expose information to cyber-attacks that result in financial losses (NITRD, 2016). Threats come from different sources such

as employees' activities or hacker's attacks (Crossler et al., 2013; Sikolia, 2013). According to Jouini et al. (2014), financial losses caused by security breaches usually cannot undergo detection. A significant number of losses, coming from smaller-scale security incidents, may cause an underestimation of information system security risk (Jouini et al., 2014). Business leaders must be knowledgeable in and be familiar with threats that may influence assets and identify their impact to determine what is required to prevent attacks through selection of appropriate countermeasures (Jouini et al., 2014).

Participants' responses to the interview questions aligned with the findings of Jouini et al. (2014) reported regarding information security and the challenges it presents to business leaders. All participants expressed, in some manner, the importance of *being in the know* and *anticipating future risks* as a vital part of risk management. IS exposes various types of threats, which can cause different levels of damage that might lead to significant financial losses (Jouini et al., 2014). The impact of information security breaches range from small and sometimes undetectable losses to the destruction of entire systems (Jouini et al., 2014). The effects of various threats vary considerably with some affecting the confidentiality or integrity of data, while others affect the availability of a system (Jouini et al., 2014). The number of data breach occurrences continues to climb worldwide and business leaders face increased challenges managing and monitoring such threats judiciously (Federal Bureau of Investigations, 2015). Participants' responses aligned with the findings of Jouini et al. of a struggle for organizations to understand what the threats are and how to obtain the necessary means to combat them. Both continue to pose a challenge for business leaders.

Comparison of Theme 4 findings with the transformational leadership conceptual framework. Results from the emergent theme related to the transformational leadership approach. The framework supports and inspires followers, promoting a team-building environment that enhances the attainment of common goals (Northouse, 2015). Transformational leadership initiatives create open communication with individual followers to achieve the organizational goal and to prevent operational security threats (Braun et al., 2013). Under the transformational leadership theory, leaders challenge followers to explore new ways to develop and implement management strategies (Braun et al., 2013). Strategic management theories, leadership, operational controls, and accountability provide the composite conceptual framework for my study (Braun et al., 2013). The findings of my study therefore align with those expected from the conceptual framework and build on previous research (Barton et al., 2016; Montesdioca & Maçada, 2015; Zia, 2015).

Summary of Findings Alignment with the Transformational Leadership Conceptual Framework

In summary**,** the four themes from my research findings relate to the transformational leadership theory. Under the transformational leadership theory, leaders challenge followers to explore new ways to develop and implement management strategies (Braun et al., 2013). Strategic management theories, leadership, operational controls, and accountability provided the composite conceptual framework for this study (Braun et al., 2013). Transformational leaders seek to transform individual goals into a

joint vision for the entire team and develop an innovative approach to emerging operational security threats (Braun et al., 2013).

Transformational leadership initiatives create open communication with individual followers to achieve organizational goals and to prevent operational security threats (Braun et al., 2013). Planned transformational leadership heightens the role of information security awareness, which influences social security behavior (Flores & Ekstedt, 2016). In conclusion, reviewing the findings from my study confirms, as did Northouse (2015) the relevance of transformational leadership and the derivative need for leadership supporting and inspiring followers in an information security culture toward achieving common goals.

Application to Professional Practice

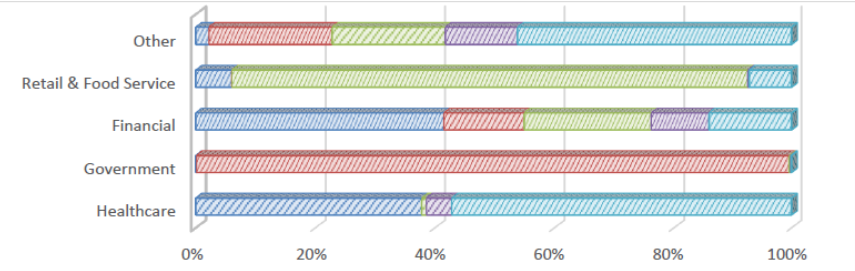
The findings and recommendations might serve as strategies for business leaders to implement and enhance operational security. Implementing strategies to prevent and mitigate operational security threats may assist business leaders in reducing the impact on the performance of the business and reduce costs transferred to the consumer. The findings and recommendations may serve as a basis for economic growth improvement that may reduce unemployment and small business losses. The results could serve as a guide to small business leaders with combating operational security breaches through improved risk management strategies and practices. Typically, small business leaders lack the resources, necessary expertise, and the manpower to combat emerging security threats (White et al., 2013). The findings of my study expand on previous research,

potentially enabling small business leaders working with limited resources to prevent and mitigate cyber security threats.

Implications for Social Change

The implication for social change from the doctoral study includes the potential development of risk management strategies small business leaders implement to prevent and mitigate security breaches that result in financial losses. I anticipated that knowledge offered in this study could: (a) contribute new insights into effective risk management strategies, (b) educate small business leaders in implementing successful risk management strategies, (c) prevent and mitigate operational security breaches, and (d) contribute to economic growth effecting the potential reduction of unemployment through reductions in small business losses.

As shown in Figure 5, SCDCA (2017) reported more than 7.6 million South Carolinians incurred effects from the 162 security breaches reported during 2011-2015. Cumulatively, 2012 represented the year with the largest number of breaches totaling 6,015,209. The total number of residents affected by breaches for the remaining years addressed in SCDCA (2017) report shown in Figure 5 are 378,940 (2011), 6,015,209 (2012), 542,710 (2013), 64,576 (2014), and 626,300 (2015) One of the most valuable business assets are consumer data (Chen, 2015). Therefore, it is imperative that business leaders implement risk management strategies, to protect consumers. Customer loyalty has a demonstrated impact on business profits and development, and paves the way for sustainability (Chen, 2015).



	Healthcare	Government	Financial	Retail & Food Service	Other
2011	330,853	5,603	4,495	34,274	3,715
2012	0	5,979,100	1,454	75	34,580
2013	6,819	10,708	2,301	491,168	31,714
2014	37,237	4,666	1,053	1,356	20,264
2015	500,153	6,457	1,521	40,828	77,341

Figure 5. Number of South Carolina residents affected by security breaches by industry from January 2011–December 2015 (SCDCA, 2017).

According to Angst, Block, D'Arcy, and Kelley (2017), the investigation of determinants of data security breaches is an important phenomenon. The importance is not simply because of the immediate or short-term effects of loss, but more importantly because of the long-lasting effects on society. SCDCA (2017) reported 750 threats during the first six months of 2017 with over half resulting from the theft of consumer data. In total, consumers reported actual losses of over $750,000, and the additional potential loss of more than $760,000, by those who did not fall victim to the threats they reported. People doubting the security of IT infrastructures and the ability of businesses to ensure the security of personal information, could cripple the financial markets (Angst et al., 2017).

Andersson and Burkart (2015) explored linkages between practices considered transgressive or piratical, their relationship to popular communication, and contribution

to social change pivotal throughout this study. The threat of digital piracy necessitates social change, as technology dependence drives a participatory democracy, and cultivates organizational innovation (Andersson & Burkart, 2015). Implementing strategies to prevent security threats may assist business leaders in reducing the impact on organizational performance and thereby lowering costs to consumers.

Recommendations for Action

Cultural enhancements in perceptions, attitudes, values, assumptions, and knowledge guide the human interaction when interacting with IS (AlHogail & Mirza, 2014). Therefore, to achieve a successful security component the recommended actions for small business leaders are to:

- Understand the potential of both internal and external computer abuse.
- Foster a positive security culture through training and awareness.
- Improve relationships between business managers and IT managers building a work environment that aligns with a positive security culture.
- Identify and respond to security issues immediately and remain proactive.
- Combat future risks through the anticipation of risks and consistent innovation.

I recommend that small business leaders review and consider the results of this study, as the use of Internet services rapidly evolves. Heightened awareness for employees and consumers is essential. Business leaders should provide periodic notifications that serve as a constant reminder of threats, require employees to attend regularly scheduled training sessions presenting illustrations of current security breach trends, and provide resources for guidance to combat challenges brought about by

evolving technologies. Future business leaders may benefit from the results of this study by developing in-depth training, monitoring business Internet activity, and implementing a risk assessment process to identify and monitor emerging security threats. Furthermore, the need for consistent innovation and proactive security measures might aid in the prevention of security threats while improving economic growth to reduce unemployment and small business losses.

The results should serve as a guide to small business leaders in combating operational security breaches through improved risk management strategies and practices. Therefore, each participant will have the ability to receive the published results and findings of the study. In addition, I will provide data from the study to the South Carolina Department of Consumer Affairs and the Department of Commerce. I will also seek to disseminate the findings of my study through academic publications, small business groups, and conferences that focus on security breach prevention and mitigation.

Recommendations for Further Research

A limitation of the study was that the findings reflected only the experiences of managers and not of employees who are responsible for addressing the phenomenon. Recommendations for further research include focusing on participants that perform daily operational functions. Identifying and exploring the experiences of insiders should be beneficial to future research. Future researchers may also consider exploring the relevance of gender and age to insider exposure to operational security threats. Continued research on the specific themes identified within this study: (a) training and awareness (b)

culture and behavioral effects, (c) policy and compliance, and d) challenges and risk management should be beneficial.

Reflections

The Walden University Doctor of Business Administration (DBA) Program has been an extremely challenging yet rewarding experience. There have been many hurdles to overcome. Undergoing devastating floods for 2 consecutive years, job loss, marriages, deaths, births, and health issues that I was not sure I would overcome are just a few of the adversities faced on this journey. It never seemed to end, but faith, a great support system, and perseverance prevailed.

Reflecting on my experiences throughout the research process, I found that business success has a common denominator, and that is communication. My doctoral study enhanced my scholarly knowledge regarding risk management strategies, computer abuse, and the Internet. Using open-ended questions with the research allowed me to conduct more in-depth follow-on discussions with participants, improving my own communication and interpersonal skills. The insights I gained from the various business leaders who participated in my research should benefit the development of my current and future careers. The doctoral study process enlightened me in a number of ways: (a) how the perform research, (b) how to broaden my knowledge through the use of literature review, (c) how leaders impact organizational culture and behavior by actions, and d) the impact organization culture has on the success of businesses and social change.

Conclusions

In order to compete in the ever-changing technological world, leaders must stay informed. The importance of budgeting for the investment in technology and keeping innovation alive within organizations are key priorities. The use of more IT security will not directly solve all operational security breaches. However, improving IT security strategies and processes can create the conditions under which IT security investments can be more effective (Angst et al., 2017). Risk management strategies must be fresh and advanced as technology evolves. To remain competitive, leaders must be proactive and aware of the changes that affect business security and sustainability.

References

Adejuwon, K. D. (2014). The dilemma of accountability and good governance for improved public service delivery in Nigeria. *Africa's Public Service Delivery and Performance Review, 1*, 25-45. Retrieved from http://www.ufh.ac.za

Al-Ahmad, W., & Mohammad, B. (2013). Addressing information security risks by adopting standards. *International Journal of Information Security Science, 2,* 28-43. Retrieved from http://www.ijiss.org/ijiss/index.php/ijiss

AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior, 49,* 567-575. doi:10.1016/j.chb.2015.03.054

AlHogail, A., & Mirza, A. (2014). Information security culture: A definition and a literature review. *2014 World Congress on Computer Applications and Information Systems (WCCAIS*), 1-7. doi:10.1109/WCCAIS.2014.6916579

Al-Yateem, N. (2012). The effect of interview recording on quality of data obtained: A methodological reflection. *Nurse Researcher*, *19*, 31–35. doi:10.7748/nr2012.07.19.4.31.c9222

Al-Zwyalif, I. M. (2013). IT governance and its impact on the usefulness of accounting information reported in financial statements. *International Journal of Business and Social Science*, *4*, 83-94. Retrieved from http://www.ijbssnet.com/

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

Aneetha, A. S., & Bose, S. (2014). Probabilistic approach for intrusion detection system-FOMC technique. *In 2014 Sixth International Conference on Advanced Computing (ICoAC), 178-183*. doi:10.1109/ICoAC.2014.7229705

Angst, C. M., Block, E. S., D'Arcy, J., & Kelley, K. (2017). When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches, *MIS Quarterly, 4*, 893-916. Retrieved from http://misq.org

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

Anyan, F. (2013). The influence of power shifts in data collection and analysis stages: A focus on qualitative research interview. *Qualitative Report*, *18*(18), 1-9. Retrieved from http://tqr.nova.edu

Arlitscha, K., & Edelmanb, A. (2014). Staying safe: Cyber security for people and organizations. *Journal of Library Administration*, *54*, 46-56. doi:10.1080101/01930826.2014.893116

Avasthi, A., Ghosh, A., Sarkar, S., & Grover, S. (2013). Ethics in medical research: General principles with special reference to psychiatry research. *Indian Journal of Psychiatry, 55*, 86-91. doi:10.4103/0019-5545.105525

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

Barker, M. (2013). Finding audiences for our research: Rethinking the issue of ethical challenges. *Communication Review, 16,* 70-80. doi:10.1080/10714421.2013.757504

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2013). Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers & Security, 39,* 145-159. doi:10.1016/j.cose.2013.05.006

Barratt, M. J., Ferris, J. A., & Lenton, S. (2015). Hidden populations, online purposive sampling, and external validity: Taking off the blindfold. *Field Methods, 27,* 3-21. doi:10.1177/1525822X14526838

Barton, K. A., Tejay, G., Lane, M., & Terrell, S. (2016). Information system security commitment: A study of external influences on senior management. *Computers & Security, 59,* 9-25. doi:10.1016/j.cose.2016.02.007

Baskarada, S. (2014). Qualitative case study guidelines. *Qualitative Report, 19*(1), 1-25. Retrieved from www.tqr.nova.edu

Baur, D., & Schmitz, H. P. (2012). Corporations and NGOs: When accountability leads to co-optation. *Journal of Business Ethics, 106,* 9-21. doi:10.1007/s10551-011-1057-9

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

Bendovschi, A. C., & Ionescu, B. S. (2015). The gap between cloud computing technology and the audit and information security. *Audit Financiar*, *13*, 115-121. Retrieved from http://revista.cafr.ro

Birkinshaw, J., Brannen, M. Y., & Tung, R. L. (2011). From a distance and generalizable to up close and grounded: Reclaiming a place for qualitative methods in international business research. *Journal of International Business Studies, 42*, 573-581. doi:10.1057/jibs.2011.19

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

Blythe, S., Wikles, L., Jackson, D., & Halcomb, E. (2013). The challenges of being an insider in storytelling research. *Nurse Researcher*, *21*, 8-13. doi:10.7748/nr2013.09.21.1.8.e333

Borrett, M., Carter, R., & Wespi, A. (2014). How is cyber threat evolving and what do organisations need to consider? *Journal of Business Continuity & Emergency Planning*, *7*, 163-171. Retrieved from https://www.henrystewartpublications.com/jbcep

Braun, S., Peus, C., Weisweiler, S., & Frey, D. (2013). Transformational leadership, job satisfaction, and team performance: A multilevel mediation model of trust. *Leadership Quarterly*, *24*, 270-283. doi:10.1016/j.leaqua.2012.11.006

Breevaart, K., Bakker, A., Hetland, J., Demerouti, E., Olsen, O. K., & Espevik, R. (2014). Daily transactional and transformational leadership and daily employee engagement. *Journal of Occupational & Organizational Psychology*, *87*(1), 138-157. doi:10.1111/joop.12041

Bryde, D., Broquetas, M., & Volm, J. M. (2013). The project benefits of building Information modeling (BIM). *International Journal of Project Management, 31*, 971-980. doi:10.1016/j.ijproman.2012.12.001

Caldwell, T. (2014). The true cost of being hacked. *Computer Fraud & Security*, *6*, 8-13. doi:10.1016/S1361-3723(14)70500-7

Campbell-Reed, E. R., & Scharen, C. (2013). Ethnography on holy ground: How qualitative interviewing is practical theological work. *International Journal of Practical Theology*, *17*, 232-259. doi:10.1515/ijpt-2013-0015

Caniëls, M. C., Lenaerts, H. K., & Gelderman, C. J. (2015). Explaining the internet usage of SMEs: The impact of market orientation, behavioural norms, motivation and technology acceptance. *Internet Research*, *25*, 358-377. doi:10.1108/IntR-12-2013-0266

Cant, M. C., & Wiid, J. A. (2013). Establishing the challenges affecting South African SMEs. *International Business & Economics Research Journal*, *12*, 707-716. Retrieved from http://www.cluteinstitute.com

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

Chatterjee, S., Sarker, S., & Valacich, J. S. (2015). The behavioral roots of information systems security: Exploring key factors related to unethical IT use. *Journal of Management Information Systems, 31*, 49-87. doi:10.1080/07421222.2014.1001257

Chen, S. (2015). Customer value and customer loyalty: Is competition a missing link. *Journal of Retailing and Consumer Services*, *22*, 107-116. doi:10.1016/j.jretconser.2014.10.007

Chen, S. (2016). Detection of fraudulent financial statements using the hybrid data mining approach. *SpringerPlus*, *5*, 1-89. doi:10.1186/s40064-016-1707

Chen, S., Zuo, Z., Huang, Z. P., & Guo, X. J. (2016). A graphical feature generation approach for intrusion detection. *MATEC Web of Conferences (Vol. 44).* Retrieved from http://www.matec-conferences.org

Cho, J. Y., & Lee, E. (2014). Reducing confusion about grounded theory and qualitative content analysis: Similarities and differences. *Qualitative Report*, *19*(32), 1-20. Retrieved from http://www.nova.edu

Coetzee, L., Preez, H. D., & Smale, N. K. (2013). South African tax incentives to alleviate unemployment: Lessons from United States of America approaches. *International Business & Economics Research Journal (Online)*, *12*, 769-780. Retrieved from http://www.cluteinstitute.com

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

Cottrell, S., & Donaldson, J. H. (2013). Exploring the opinions of registered nurses working in a clinical transfusion environment on the contribution of e-learning to personal learning and clinical practice: Results of a small-scale educational research study. *Nurse Education in Practice, 13,* 221-227. doi:10.1016/j.nepr.2013.01.014

Cronin, C. (2014). Using case study research as a rigorous form of inquiry. *Nurse Researcher, 21,* 19-27. doi:10.7748/nr.21.5.19.e1240

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32,* 90-101. doi:10.1016/j.cose.2012.09.010

Cruz, E. V., & Higginbottom, G. (2013). The use of focused ethnography in nursing research. *Nurse Researcher, 20,* 36-43. Retrieved from http://journals.rcni.com

Dahnil, M. I., Marzuki, K. M., Langgat, J., & Fabeil, N. F. (2014). Factors influencing SMEs adoption of social media marketing. *Procedia - Social and Behavioral Sciences, 148,* 119-126. doi:10.1016/j.sbspro.2014.07.025

D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security, 22,* 474-489. doi:10.1108/IMCS-08-2013-0057

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems, 31,* 285-318. doi:10.1080/07421222.2014.1001257

Da Veiga, A. (2016). Comparing the information security culture of employees who had read the information security policy and those who had not: Illustrated through an empirical study. *Information & Computer Security, 24,* 139-151. doi:10.1108/ICS-12-2015-0048

Da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security, 49,* 162-176. doi:10.1016/j.cose.2014.12.006

Darawsheh, W. (2014). Reflexivity in research: Promoting rigour, reliability and validity in qualitative research. *International Journal of Therapy & Rehabilitation, 21,* 560–568. doi:10.12968/ijtr.2014.21.12.560

De Jaegher, H., Pieper, B., Clénin, D., & Fuchs, T. (2016). Grasping intersubjectivity: An invitation to embody social interaction research. *Phenomenology and the Cognitive Sciences, 1,* 1-33. doi:10.1007/s11097-016-94698

De Massis, A., & Kotlar, J. (2014). The case study method in family business research: Guidelines for qualitative scholarship. *Journal of Family Business Strategy, 5,* 15-29. doi:10.1016/j.jfbs.2014.01.007

Denscombe, M. (2014). *The good research guide: For small-scale social research* projects. New York, NY: McGraw-Hill

Department of Health, E. (2014). The Belmont Report: Ethical principles and guidelines for the protection of human subjects of research. *Journal of the American College of Dentists, 81,* 4-13. Retrieved from http://www.ncbi.nlm.nih.gov

Dhillon, G., Syed, R., & Pedron, C. (2016). Interpreting information security culture: An organizational transformation case study. *Computers & Security, 56,* 63-69. doi:10.1016/j.cose.2015.10.001

Doody, O., & Noonan, M. (2013). Preparing and conducting interviews to collect data. *Nurse Researcher, 20,* 28-32. Retrieved from http://journals.rcni.com

Dunn-Cavelty, M. (2013). From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. *International Studies Review, 15,* 105-122. doi:10.1111/misr.12023.

Dworkin, S. L. (2012). Sample size policy for qualitative studies using in-depth interviews. *Archives of Sexual Behavior, 41,* 1319-1320. doi:10.1007/s105080120016-6

Earley, M. A. (2014). A synthesis of the literature on research methods education. *Teaching in Higher Education, 19,* 242-253. doi:10.1080/13562517.2013.860105

Elo, S., Kaariainen, M., Kanste, O., Polkki, T., Utriainen, K., & Kyngas, H. (2014). Qualitative content analysis. *Sage Open, 4*(1), 1-10. doi:10.1177/2158244014522633

Elsawah, S., Guillaume, J. H., Filatova, T., Rook, J., & Jakeman, A. J. (2015). A methodology for eliciting, representing, and analyzing stakeholder knowledge for decision making on complex socio-ecological systems: From cognitive maps to agent-based models. *Journal of Environmental Management, 151,* 500-516. doi:10.1016/j.jenvman.2014.11.028

Emerson, R. W. (2015). Convenience sampling, random sampling, and snowball sampling: How does sampling affect the validity of research? *Journal of Visual Impairment & Blindness*, *109*, 164-168. Retrieved from http://www.afb.org

Eriksson, J., & Giacomello, G. (2006). The information revolution, security, and international relations: (IR) relevant theory. *International Political Science Review*, *27*, 221-244. doi:10.1177/0192512106064462

Erlingsson, C., & Brysiewicz, P. (2013). Orientation among multiple truths: An introduction to qualitative research. *African Journal of Emergency Medicine*, *3*, 92-99. doi:10.1016/j.afjem.2012.04.005

Fazlida, M., & Said, J. (2015). Information security: Risk, governance and implementation setback. *Procedia Economics and Finance*, *28*, 243-248. doi:10.1016/S2212-5671(15)01106-5

Federal Bureau of Investigations. (2015). *Business e-mail compromise*. Retrieved from http://www.fbi.gov

Federal Bureau of Investigations. (2016). *Business e-mail compromise*: *The 3.1 billion dollar scam.* Retrieved from http://www.fbi.gov

Feng, N., Wang, H. J., & Li, M. (2014). A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis. *Information Sciences*, *256*, 57-73. doi:10.1016/j.ins.2013.02.036

Fiske, S. T., & Hauser, R. M. (2014). Research method: Protecting human research participants in the age of big data. *Proceedings of the National Academy of Sciences*, *11*, 13675-13676. doi:10.1073/pnas.1414626111

Flores, W. R., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security, 43,* 90-110. doi:10.1016/j.cose.2014.03.004

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

Foley, D., & O'Connor, A. J. (2013). Social capital and the networking practices of indigenous entrepreneurs. *Journal of Small Business Management, 51,* 276-296. doi:10.1111/jsbm.12017

Francis, J. J., Johnston, M., Robertson, C., Glidewell, L., Entwistle, V. Eccles, M. P., & Grimshaw, J. M. (2010). What is an adequate sample size? Operationalizing data saturation for theory-based interview studies. *Psychology and Health, 25,* 1229-1245. doi:10.1080/08870440903194015

Franco, A. R., Mannell, M. V., Calhoun, V. D., & Mayer, A. R. (2013). Impact of analysis methods on the reproducibility and reliability of resting-state networks. *Brain Connectivity, 3,* 363-374. doi:10.1089/brain.2012.0134

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

Galliers, R. D., & Leidner, D. E. (2014). *Strategic information management: Challenges and strategies in managing information systems*. New York, NY: Routledge.

Gennaro, S. (2014). Conducting important and ethical research. *Journal of Nursing Scholarship, 46*, 73. Retrieved from http://www.nursingsociety.org

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

Gergen, K. J., Josselson, R., & Freeman, M. (2015). The promises of qualitative inquiry. *American Psychologist, 70*, 1-9. doi:10.1037/a0038587

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking qualitative rigor in inductive research notes on the Gioia methodology. *Organizational Research Methods, 16*, 15-31. doi:10.1177/1094428112452151

Goo, J., Yim, M. S., & Kim, D. J. (2014). A path to successful management of employee security compliance: An empirical study of information security climate. *Transactions on Professional Communication, 57*, 286-308, IEEE. doi:10.1109/TPC.2014.2374011

Groeneveld, S., Tummers, L., Bronkhorst, B., Ashikali, T., & Van Thiel, S. (2015). Quantitative methods in public administration: Their use and development through time. *International Public Management Journal, 18*, 61-86. doi:10.1080/10967494.2014.972484

Gu, V. C., Hoffman, J. J., Cao, Q., & Schniederjans, M. J. (2014). The effects of organizational culture and environmental pressures on IT project performance: A moderation perspective. *International Journal of Project Management, 32,* 1170-1181. doi:10.1016/j.ijproman.2013.12.003

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

Haahr, A., Norlyk, A., & Hall, E. (2013). Ethical challenges embedded in qualitative research interviews with close relatives. *Nursing Ethics, 2,* 6-15. doi:10.1177/0969733013486370

Haigh, T., Russell, A. L., & Dutton, W. H. (2015). Histories of the Internet: Introducing a special issue of information & culture. *Information & Culture*, *50,* 143-159. doi:10.7560/IC50201

Harris, F., & Lyon, F. (2013). Transdisciplinary environmental research: Building trust across professional cultures. *Environmental Science & Policy, 31,* 109-119. doi:10.1016/j.envsci.2013.02.006

Harvey, L. (2015). Beyond member checking: A dialogic approach to the research interview. *International Journal of Research & Method in Education*, *38*, 23-38. doi:10.1080/1743727X.2014.914487

Hill, R. (2015). Dealing with cyber security threats: International cooperation, ITU, and WCIT. In Cyber Conflict: *Architectures in Cyberspace (CyCon), 2015 7th International Conference,* 119-134. doi:10.1109/CYCON.2015.7158473

Hills, M., & Anjali, A. (2017). A human factors contribution to countering insider threats: Practical *prospects from a novel approach to warning and avoiding. Security Journal, 30,* 142-152. doi:10.1057/sj.2015.36

Hoover, S. M., & Morrow, S. L. (2015). Qualitative researcher reflexivity: A follow-up study with female sexual assault survivors. *Qualitative Report, 20,* 1476. Retrieved from http://www.nova.edu

Houghton, C., Casey, D., Shaw, D., & Murphy, K. (2013). Rigour in qualitative case-study research. *Nurse Researcher, 20,* 12-17. doi:10.7748/nr2013.03.20.4.12.e326

Hussein, M. E., Hirst, S., Shaw, D., & Murphy, K. (2014). Using grounded theory as a method of inquiry: Advantages and disadvantages. *Qualitative Report, 19*(13), 1-15. Retrieved from www.nova.edu

Hynes, M. (2013). The practices of technology: Putting society and technology in their place. *International Journal of Technology, Knowledge and Society. 8,* 37-55. Retrieved from http://ijt.cgpublisher.com

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management, 51,* 69-79. doi:10.1016/j.im.2013.10.001

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

Ishak, N. M., & Bakar, A. Y. A. (2014). Developing sampling frame for case study: Challenges and conditions. *World Journal of Education, 4,* 29-35. doi:10.5430/wje.v4n3p29

James, M. L. (2013). Sustainability and integrated reporting: Opportunities and strategies for small and midsize companies. *Entrepreneurial Executive*, *18*, 17-28. Retrieved from http://www.alliedacademies.org

Järveläinen, J. (2013). IT incidents and business impacts: Validating a framework for continuity management in information systems. *International Journal of Information Management*, *33*, 583-590. doi:10.1016/j.ijinfomgt.2013.03.001

Jordan, S. R. (2014). The innovation imperative: An analysis of the ethics of the imperative to innovate in public sector service delivery. *Public Management Review*, *16*, 67-89. doi:10.1080/14719037.2013.790274

Jouini, M., Rabai, L. B. A., & Aissa, A. B. (2014). Classification of security threats in information systems. *Procedia Computer Science*, *32*, 489-496. doi:10.1016/j.procs.2014.05.452

Kallio, H., Pietilä, A. M., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: Developing a framework for a qualitative semi-structured interview guide. *Journal of Advanced Nursing*, 72, 2954-2975. doi:10.1111/jan.13031

Kamil, M. L., Mosenthal, P. B., Pearson, P. D., & Barr, R. (Eds.). (2014). *Handbook of reading research*. New York, NY: Routledge.

Kanatov, M., Atymtayeva, L., & Yagaliyeva, B. (2014). Expert systems for information security management and audit: Implementation phase issues. *In Soft Computing and Intelligent Systems (SCIS), 2014 Joint 7th International Conference on and Advanced Intelligent Systems (ISIS), 15th International Symposium on*, 896-900. doi:10.1109/SCIS-ISIS.2014.7044702

Karanja, E., & Zaveri, J. (2014). Ramifications of the Sarbanes Oxley (SOX) act on IT governance. *International Journal of Accounting and Information Management*, *22*, 134-145. doi:10.1108/IJAIM-02-2013-0017

Kearney, W. D., & Kruger, H. A. (2016). Can perceptual differences account for enigmatic information security behaviour in an organisation? *Computers & Security*, *61*, 46-58. doi:10.1016/j.cose.2016.05.006

Kello, L. (2013). The meaning of the cyber revolution: Perils to theory and statecraft. *International Security*, *38*, 7-40. doi:10.1162/ISEC_a_00138

Kuhnert, K. W., & Lewis, P. (1987). Transactional and transformational leadership: A constructive/developmental analysis. *Academy of Management Review*, *12*, 648-657. Retrieved from http://aom.org

Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cyber crime on the financial sector. *Computers & Security, 45*, 58-74. doi:10.1016/j.cose.2014.05.006

Lauridsen, E. I., & Higginbottom, G. (2014). The roots and development of constructivist grounded theory. *Nurse Researcher*, *21*, 8-13. doi:10.7748/nr.21.5.8.e1208

Lecic-Cvetkovic, D., Omerbegovic-Bijelovic, J., Zaric, S., & Janicic, R. (2016). E-banking application in business companies–A case study of Serbia. *Information Development*, *32*, 762-776. doi:10.1177/0266666914568652

Lee, B., Riche, N. H., Isenberg, P., & Carpendale, S. (2015). More than telling a story: A closer look at the process of transforming data into visually shared stories. *IEEE Computer Graphics and Applications*, *35*, 84-90. doi:10.1109/MCG.2015.99

Lee, C., Jung, D., & Lee, K. (2013). A Survey on Security Threats and Security Technology Analysis for Secured Cloud Services. *International Journal of Security and Its Applications*, *7*, 21-30. doi:10.14257/ijsia.2013.7.6.03

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

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

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. Newbury Park, CA; Sage.

Lim, J. S., Maynard, S. B., Ahmad, A., & Chang, S. (2015). Information security culture: Towards an instrument for assessing security management practices. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, *5*, 31-52. doi:10.4018/IJCWT.2015040103

Lin, W. C., Ke, S. W., & Tsai, C. F. (2015). CANN: An intrusion detection system based on combining cluster centers and nearest neighbors. *Knowledge-Based Systems*, *78*, 13-21. doi:10.1016/j.knosys.2015.01.009

Line, M. B., & Albrechtsen, E. (2016). Examining the suitability of industrial safety management approaches for information security incident management. *Information & Computer Security, 24*, 20-37. doi:10.1108/ICS-01-2015-0003

LinkedIn®. (2016). *Company directory*. Retrieved from http://www.linkedin.com

Mackenzie, C. A., Ricker, B., Christensen, J., Heller, E., Kagan, E., Osano, P. M., & Turner, S. (2013). Dear diary revisited: Reflecting on collaborative journaling. *Journal of Geography in Higher Education, 37*, 480-486. doi:10.1080/03098265.2013.868080

Majumdar, S. (2013). Growth strategy in entrepreneur managed small organizations: A study in auto component manufacturing organizations in central India. *South Asian Journal of Management, 20*, 31-55. Retrieved from http://www.sajmamdisa.org

Malterud, K. (2001). Qualitative research: Standards, challenges, and guidelines. *The Lancet, 358*, 483-488. doi:10.1016/S0140-6736(01)05627-6

Marshall B., Cardon, P., Poddar, A., & Fontenot, R. (2013). Does sampling size matter in qualitative research? A review of qualitative interviews in IS research. *Journal of Computer Information Systems, 54*, 11-22. Retrieved from www.iacis.org

Mayoh, J., & Onwuegbuzie, A. J. (2013). Toward a conceptualization of mixed methods phenomenological research. *Journal of Mixed Methods Research, 9*, 91-107. doi:10.1177/1558689813505358

Mellado, D., & Rosado, D. G. (2012). An overview of current information systems security challenges and innovations JUCS Special Issue. *Journal of Universal Computer Science*, *18*, 1598-1607. Retrieved from http://www.jucs.org

Merriam, S. B. (2014). *Qualitative research: A guide to design and implementation* (2nd ed.). San Francisco, CA: John Wiley & Sons.

Mitchell, G. (2015). Use of interviews in nursing research. *Nursing Standard*, *29*, 44-48. doi:10.7748/ns.29.43.44.e8905

Montesdioca, G. P. Z., & Maçada, A. C. G. (2015). Measuring user satisfaction with information security practices. *Computers & Security*, *48*, 267-280. doi:10.1016/j.cose.2014.10.015

Moura, J., & Hutchison, D. (2016). Review and analysis of networking challenges in cloud computing. *Journal of Network and Computer Applications*, *60*, 113-129. doi:10.1016/j.jnca.2015.11.015

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

Naia, A., Baptista, R., Januário, C., & Trigo, V. (2014). Entrepreneurship education literature in the 2000s. *Journal of Entrepreneurship Education*, *17*, 118-142. Retrieved from http://www.readperiodicals.com

National Institute of Standards and Technology. (2013). *Special Publication 800-63-2 Electronic Authentication Guideline.* Retrieved from https://www.nist.gov

Nazareth, D. L., & Choi, J. (2015). A system dynamics model for information security management. *Information & Management, 52,* 123-134. doi:10.1016/j.im.2014.10.009

Networking and Information Technology Research and Development Program. (2015). *Report to the President and Congress Ensuring Leadership in Federally Funded Research and Development in Information Technology.* Retrieved from https://www.nitrd.gov/

Networking and Information Technology Research and Development Program. (2016). *The National Cybersecurity Center of Excellence (NCCoE) Project Description on the topic of Multifactor Authentication for e-Commerce.* Retrieved from https://nccoe.nitrd.gov

Networking and Information Technology Research and Development Program. (2016). *Multifactor Authentication for e-Commerce: Online Authentication for the Retail Sector*. Retrieved from https://www.nitrd.gov

Nijhawan, L. P., Janodia, M. D., Muddukrishna, B. S., Bhat, K. M., Bairy, K. L., Udupa, N., & Musmade, P. B. (2013). Informed consent: Issues and challenges. *Journal of Advanced Pharmaceutical Technology Research, 4*, 134-140. doi:10.4103/2231-4040.116779

Nishimura, A., Carey, J., Erwin, P. J., Tilburt, J. C., Murad, M. H., & McCormick, J. B. (2013). Improving understanding in the research informed consent process: A systematic review of 54 interventions tested in randomized control trials. *BMC Medical Ethics*, *14*(1), 1-15. doi:10.1186/1472-6939-14-28

Noor, F. M. (2013). Choice of business aims and strategies by small business enterprises in developing countries. *International Journal of Business and Social Science, 4*, 247-255. Retrieved from http://ijbssnet.com

Northouse, P. G. (2015). *Leadership: Theory and practice*. Thousand Oaks, CA: Sage Publications.

Nykänen, R., & Kärkkäinen, T. (2016). *Supporting cyber resilience with semantic wiki. In Proceedings of the 12th International Symposium on Open Collaboration, 21*. Retrieved from http://www.opensym.org

Oberoi, D. V., Jiwa, M., McManus, A., Hodder, R. (2015). Barriers to help-seeking in men diagnosed with benign colorectal diseases. *American Journal of Health Behavior, 39,* 22-33. doi:10.5993/AJHB.39.1.3

O'Brien, B. C., Harris, I. B., Beckman, T. J., Reed, D. A., & Cook, D. A. (2014). Standards for reporting qualitative research: A synthesis of recommendations. *Academic Medicine, 89,* 1245-1251. doi:10.1097/ACM.0000000000000388

Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security, 56,* 83-93. doi:10.1016/j.cose.2015.10.002

Parra, F., & Hall, L. L. (2014). A nomological network analysis of research on information security management systems. *In 2014 47th Hawaii International Conference on System Sciences*, 4336-4345, IEEE. doi:10.1109/HICSS.2014.536

Patel, A., Taghavi, M., Bakhtiyari, K., & JúNior, J. C. (2013). An intrusion detection and prevention system in cloud computing: A systematic review. *Journal of Network and Computer Applications, 36,* 25-41. doi:10.1016/j.jnca.2012.08.007

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

Pawlik, A. (2014). Safeguarding the future of the internet. *Computer Fraud & Security, 6,* 13-15. doi:10.1016/S1361-3723(14)70501-9

Pettigrew, A. M. (2013). The conduct of qualitative research in organizational settings. *Corporate Governance: An International Review, 21*, 123-126. doi:10.1111/j.1467-8683.2012.00925.x

Pfleeger, S. L., Sasse, M. A., & Furnham, A. (2014). From weakest link to security hero: Transforming staff security behavior. *Journal of Homeland Security & Emergency Management, 11*, 489-510. doi:10.1515/jhsem-2014-0035

Pierre, E. A. S., & Jackson, A. Y. (2014). Qualitative data analysis after coding. *Qualitative Inquiry, 20,* 715-719. doi:10.1177/1077800414532435

Ponterotto, J. G. (2014). Best practices in psychobiographical research. *Qualitative Psychology, 1,* 77-90. doi:10.1037/qup0000005

Potter, S. (2013). Learning to value stories: A review of narrative inquiry. *The Qualitative Report, 18*(18), 1-3. Retrieved from www.nova.edu

Price Waterhouse Cooper. (2013). *2013 information security breaches survey*. Retrieved from http://www.pwc.co.uk

Ramayah, T., Ling, N. S., Taghizadeh, S. K., & Rahman, S. A. (2015). Factors influencing SMEs website continuance intention in Malaysia. *Telematics and Informatics*, *33*, 150-164. doi:10.1016/j.tele.2015.06.007

Rice, E., Holloway, I. W., Barman-Adhikari, A., Fuentes, D., Brown, C. H., & Palinkas, L. A. (2014). A mixed methods approach to network data collection. *Field Methods*, *26*, 252-268. doi:10.1177/1525822X13518168

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

Roratto, R., & Dotto-Dias, E. (2014). Security information in production and operations: A study on audit trails in database systems. *Journal of Information Systems & Technology Management*, *11*, 717-734. doi:10.4301/S1807-17752014000300010

Rosenfeld, J., Gatten, R., & Scales, B. J. (2013). Qualitative analysis of student assignments: A practical look at ATLAS. *Reference Services Review*, *41*, 134-147. doi:10.1108/01409171211210154

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

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

Saunders, B., Kitzinger, J., & Kitzinger, C. (2015). Participant anonymity in the internet age: from theory to practice. *Qualitative Research in Psychology*, *12*, 125-137. doi:10.1080/14780887.2014.948697

Setia, P., Venkatesh, V., & Joglekar, S. (2013). Leveraging digital technologies: How information quality leads to localized capabilities and customer service performance. *MIS Quarterly*, *37*, 565-590. Retrieved from http://misq.org

Shin, S., Lee, S., Kim, H., & Kim, S. (2013). Advanced probabilistic approach for network intrusion forecasting and detection. *Expert Systems with Applications*, *40*, 315-322. doi:10.1016/j.eswa.2012.07.057

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, *49*, 177-191. doi:10.1016/j.cose.2015.01.002

Sikolia, D. (2013). A thematic review of user compliance with information security policies literature. *Journal of Digital Forensics, Security, & Law*, *1*, 101-104. Retrieved from http://www.jdfsl.org

Simon, M. K., & Goes, J. (2013). Scope, limitations, and delimitations. *Diss. Sch. Res. Recipes Success*. Retrieved from http://dissertationrecipes.com

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

Soluade, O. A., & Opara, E. U. (2014). Security breaches, network exploits and vulnerabilities: A conundrum and an analysis. *International Journal of Cyber-Security and Digital Forensics, 3*, 246-261. doi:10.17781/P001383

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Information & Computer Security, 23*, 200-217. doi:10.1108/ICS-04-2014-0025

Sousa, D. (2014). Validation in qualitative research: General aspects and specificities of the descriptive phenomenological method. *Qualitative Research in Psychology, 11*, 211-227. doi:10.1080/14780887.2013.853855

South Carolina Department of Consumer Affairs. (2016). *National consumer protection week.* Retrieved from www.consumer.sc.gov

South Carolina Department of Consumer Affairs. (2017). *Over 700 Scams Reported to SCDCA in the First Half of 2017.* Retrieved from www.consumer.sc.gov

Spears, J. L., Barki, H., & Barton, R. R. (2013). Theorizing the concept and role of assurance in information systems security. *Information & Management, 50*, 598-605. doi:10.1016/j.im.2013.08.004

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. (2013). Information security professionals' perceptions about the relationship between the information security and internal audit functions. *Journal of Information Systems, 27*, 65-86. doi:10.2308/isys-50510

Stone, A. G., Russell, R. F., & Patterson, K. (2004). Transformational versus servant leadership: A difference in leader focus. *Leadership & Organization Development Journal*, *25*, 349-361. doi:10.1108/01437730410538671

Toles, M., & Barroso, J. (2014). Qualitative approaches to research. *Nursing research: Methods and critical appraisal for evidence-based practice* (8th ed.). St Louis, MO: Elsevier.

Trafimow, D. (2014). Considering quantitative and qualitative issues together. *Qualitative Research in Psychology*, *11*, 15–24. doi:10.1080/14780887.2012.743202

Tsohou, A., Karyda, M., & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: recommendations for information security awareness programs. *Computers & security*, *52*, 128-141. doi:10.1108/MRR-04-2013-0085

Vaz, S., Falkmer, T., Passmore, A. E., Parsons, R., & Andreou, P. (2013). The case for using the repeatability coefficient when calculating test–retest reliability. *PLoS One*, *8*(1), 1-7. doi:10.1371/journal.pone.0073990

Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS Quarterly*, *37*, 21-54. Retrieved from http://www.misq.org

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

Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, *23*, 371-376. doi:10.1016/j.cose.2004.05.002

White, G. L., Hewitt, B., & Kruck, S. E. (2013). Incorporating global information security and assurance in I.S. education. *Journal of Information Systems Education*, *24*, 11-16. Retrieved from http://jise.org

Wijnhoven, F., & Brinkhuis, M. (2015). Internet information triangulation: Design theory and prototype evaluation. *Journal of the Association for Information Science and Technology*, *66*, 684-701. doi:10.1002/asi.23203

Williams, P. A. (2013). Information security governance: A risk assessment approach to health information systems protection. *Studies in Health Technology & Informatics*, *19*, 186-206. doi:10.3233/978-1-61499-291-2-186

Williams, S., Hardy, C., & Holgate, J. (2013). Information security governance practices in critical infrastructure organizations: A socio-technical and institutional logic perspective. *Electronic Markets*, *23*, 341-354. doi:10.1007/s12525-013-0137-3

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly*, *37*, 1-20. Retrieved from http://misq.org

Woods, M., Paulus, T., Atkins, D. P., & Macklin, R. (2015). Advancing qualitative research using qualitative data analysis software (QDAS): Reviewing potential versus practice in published studies using ATLAS.ti and NVivo. *Social Science Computer Review*, *34*, 597-617. doi:10.1177/0894439315596311

Wu, D., & Shan, S. (2015). Meta-analysis of network information security and web data mining techniques. *International Conference on Information Sciences, Machinery, Materials and Energy (ICISMME)*, 1974-1977. Retrieved from http://www.atlantis-press.com

Yaokumah, W., & Brown, S. (2014). An empirical examination of the relationship between information security/business strategic alignment and information security governance domain AREAS. *Journal of Business Systems, Governance & Ethics, 9*, 50-65. Retrieved from http://www.jbsge.vu.edu

Ye, Y., Wandong, C., & Nan, F. (2016). Network & information system security risk assessment technology. *International Bhurban Conference on Applied Sciences & Technology*, 397-401. doi:10.1109/IBCAST.2016.7429909

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

Yin, R. K. (2013). Validity and generalization in future case study evaluations. *Evaluation, 19*, 312-332. doi:10.1177/1356389013497081

Yin, R. K. (2014). *Case study research: Designs and methods* (5th ed.). Thousand Oaks, CA: Sage Publications.

Yu, H., Abdullah, A., & Saat, R. M. (2014). Overcoming time and ethical constraints in the qualitative data collection process: A case of information literacy research. *Journal of Librarianship and Information Science, 46*, 243-257. doi:10.1177/0961000614526610

Zafar, H., Ko, M. S., & Osei-Bryson, K. M. (2015). The value of the CIO in the top management team on performance in the case of information security breaches. *Information Systems Frontiers*, *18*, 1205-1215. doi:10.1007/s10796-015-9562-5

Zia, T. A. (2015). Organisations capability and aptitude towards IT security governance. *5th International Conference on IT Convergence and Security (ICITCS*), 1-4. doi:10.1109/ICITCS.2015.7293005

Zivkovic, J. (2012). Strengths and weaknesses of business research methodologies: Two disparate case studies. *Business Studies Journal*, *4*, 91-99. Retrieved from http://www.alliedacademies.org

Appendix A: Recruitment Letter for Study Participants

June 30, 2017

Re: A Doctoral Study of Potential Interest

Dear Colleagues:

My name is Nancy Larrimore and I am currently a graduate student at Walden University pursuing a doctoral degree in Business Administration with an Accounting specialization. I am conducting research on emerging operational security threats. My study is entitled: "Risk Management Strategies to Prevent and Mitigate Emerging Operational Security Threats". I am interested in conducting the study to explore risk management strategies to prevent operational security breaches producing financial losses.

I am seeking to interview small business leaders who fit the following criteria:

- Working in a small business in South Carolina.
- Employed in a full-time, manager position with a minimum of 1-year experience working with successful risk management strategies.
- Working directly with the implementation of risk management strategies to prevent operational security threats that produce financial losses

The participants' experiences have been determined to provide the researcher with unique perspectives to this research. Participants who choose to become a participant in the study will be asked to do so in a face-to-face interview. The results and findings will be shared with participants, other scholars, and the organization senior leadership. All responses will be categorized, and no names will be attached in any form to the results. Confidentiality is assured through protocol established by the Walden University Institutional Review Board (IRB).

Individuals, who met the above criteria and are interested in participating in the study, are asked to contact me at XXX-XXX-XXXX or across email at XXX@WaldenU.edu. Participation in this study is obviously voluntary.

Thank you for your time and consideration.

Sincerely,

Nancy P. Larrimore

Appendix B: Letter of Cooperation

Community Research Partner Name

Contact Information

Date:

Dear Researcher Name,

Based on my review of your research proposal, I give permission for you to conduct the study entitled "Risk Management Strategies to Prevent Emerging Operational Security Threats" within the [Insert Name of Community Partner]. As part of this study, I authorize you to access supporting documentation of risk management operating procedures addressing the research question: What risk management strategies do small business leaders use to prevent operational security threats that produce financial losses? Individuals' participation will be voluntary and at their discretion.

We understand that our organization's responsibilities include: [Insert a description of all personnel, rooms, resources, and supervision that the partner will provide]. We reserve the right to withdraw from the study at any time if our circumstances change.

I confirm that I am authorized to approve research in this setting and that this plan complies with the organization's policies.

I understand that the data collected will remain entirely confidential and may not be provided to anyone outside of the student's supervising faculty/staff without permission from the Walden University IRB.

Sincerely,
Authorization Official
Contact Information

Appendix C: Interview Protocol

The purpose of the interview is to explore what risk management strategies are relevant for business leaders to prevent and mitigate operational security breaches. Business leaders of small to medium businesses are interviewed and each participant asked the same questions in the protocol below:

1. I will introduce myself to the participant as a doctoral student at Walden University and explain the purpose and time of the interview.

2. A copy of the consent form will be provided to the participant to read and sign prior to the interview process. Once signed only one participant retained a copy.

3. I will remind the participant the interview will be audio-recorded. The interview will start with the following background information:
   a. Education background
   b. When did you start your business?
   c. How many employees do you have?

   The research questions will follow.
   1. What risks related to the operational security of financial data are associated with your business use of the Internet?
   2. Which effective risk management strategies have you implemented to achieve operational security?
   3. How do you measure the effectiveness of these strategies?
   4. What are some of the challenges you have encountered when responding to operational security threats, and how did you address the challenges?
   5. How where the challenges to implementing the strategies for risk management addressed?
   6. What additional information on developing and implementing strategies to prevent security threats can you add that would be valuable to the study?

4. I will thank the interviewer for participating, stop the audio recording, and conclude the interview.

Appendix D: Introductory Letter

Nancy Larrimore
405 Harbison Blvd
Columbia SC, 29212
June XX, 20XX

Dear [Insert Participants Name]:

As part of my doctoral study research at Walden University, I would like to invite you to participate in a research study I am conducting to explore risk management strategies to prevent emerging operational security threats for small to medium businesses in South Carolina. I contacted you to participate because you are a small to medium business leader in South Carolina. The data collected will be confidential, and participation is voluntary.

If you agree to participate in the study, please review the enclosed consent form carefully and ask any questions you feel are necessary. My role as a researcher is to ensure aspects of the research are clear to each participant before the participant consent to the interview. The interview should last approximately 60 minutes and will include questions about your strategies and experiences pertaining to reducing operational security threats and their consequences. I will record the interview, and you will have the opportunity to review the transcribed interview for accuracy prior to inclusion in the study. Your participation is valuable to the success of the study. Thank you for your time and cooperation.

Thank you for your time and consideration.

Sincerely,

Nancy P. Larrimore